Ville Uusitupa

KYBERTURVALLISUUDEN KIIHDYTTÄJÄ – TIETOTURVAKONSULTOINTIYHTIÖIDEN COVID-19-DISKURSSIN HABERMASILAINEN ANALYYSI

JYVÄSKYLÄN YLIOPISTO
INFORMAATIOTEKNOLOGIAN TIEDEKUNTA
2021

TIIVISTELMÄ

Uusitupa, Ville
Kyberturvallisuuden kiihdyttäjä – Tietoturvakonsultointiyhtiöiden COVID-19 diskurssin habermasilainen analyysi
Jyväskylä: Jyväskylän yliopisto, 2021, 71 s.
Kyberturvallisuus, pro gradu -tutkielma
Ohjaaja: Vuorinen, Jukka

Maaliskuun 11. päivä 2020 Maailman terveysjärjestö WHO julisti COVID-19-koronavirustaudin globaaliksi epidemiaksi eli pandemiaksi. Pandemian myötä ihmisten liikkumista ja kokoontumista on rajoitettu useissa maissa ympäri maapalloa merkittävästi tämän kirjoitushetkellä jo yli vuoden ajan. Tällä on ollut useiden organisaatioiden päivittäiselle toiminnalle myös tuntuvaa vaikutusta, kun työntekijät ovat konttorille saapumiseen sijaan viranomaisten määräysten ja suositusten mukaisesti hoitaneet työtehtäviään kotoaan tai muusta etätyöskentelypisteestä käsin. Tässä pro gradu -tutkielmassa tutkitaan kahden tietoturvakonsultointiyhtiön, Deloitten ja PwC:n, COVID-19-pandemiaa ja kyberturvallisuutta käsittelevien verkkojulkaisujen (artikkelit, blogit ja raportit) tuottamaa kuvaa ja merkityksiä COVID-19-pandemiasta organisaatioiden kyberturvallisuudelle. Tutkielman päätutkimuskysymyksenä on millaiseksi COVID-19-pandemian merkitys ja vaikutus organisaatioiden kyberturvallisuudelle tutkimusaineistossa kuvataan. Lisäksi tutkielmassa analysoidaan sitä, mitä mahdollisia seurauksia ja vaikutuksia tutkimusaineistossa olevalla kielenkäytöllä on ymmärryksellemme kyberturvallisuudesta COVID-19-pandemian aikana sekä millaisia kyberturvallisuuteen liittyviä valtasuhteita julkaisut tuottavat ja ylläpitävät. Tutkielma perustuu sosiaalisen konstruktionismin käsitykseen todellisuudesta, jossa sosiaalinen todellisuus, kuten ymmärryksemme turvallisuudesta, nähdään rakentuvan ihmisten välisessä vuorovaikutuksessa esimerkiksi kielenkäytön kautta. Tutkielmassa käytetty tutkimusmenetelmä on habermasilainen diskurssianalyysi, jossa tutkimusainestoa on analysoitu Jürgen Habermasin neljän kommunikaation pätevyysvaatimuksen – totuuden, oikeellisuuden, vilpittömyyden ja ymmärrettävyyden – kautta. Tutkielman keskeisimpänä johtopäätöksenä COVID-19-pandemia näyttäytyy tutkimusaineistossa organisaatioille kyberriskejä kasvattaneena ennalta-arvaamattomana murroksena, jossa pärjäämiseksi organisaatioiden tulee päivittää tietoturvakyvykkyyksiään sekä prosessien että teknologian osalta. Lisäksi tutkimusaineiston havaittiin tuottavan kyberturvallisuudesta käsitystä tietoturva-asiantuntijoiden ja -päättäjien valtakenttänä, jolla organisaatioiden henkilöstö näyttäytyy lähinnä organisaatioiden riskejä kasvattavana toimijana.

Asiasanat: kyberturvallisuus, COVID-19, tietoturvakonsultointi, sosiaalinen konstruktionismi, diskurssianalyysi, Jürgen Habermas

ABSTRACT

Uusitupa, Ville
The Accelerator of Cyber Security – A Habermasian Analysis of Cyber Security Consulting Firms' COVID-19 Discourse
Jyväskylä: University of Jyväskylä, 2020, 71 pp.
Cyber Security, Master's Thesis
Supervisor: Vuorinen, Jukka

On 11th of March 2020 World Health Organization declared COVID-19 as a global pandemic. Due to pandemic there has been significant restrictions on people's movement and gatherings in countries around the globe. COVID-19 has also had an impact on day-to-day operations of several organizations. As ordered and recommended by the local authorities, many organization has moved to remote working mode. In this master's thesis the focus is on the organizational cyber security discourse of COVID-19. This is done by analyzing the publicly available COVID-19 themed cyber security publications (articles, blogs and reports) of two cyber security consulting firms, Deloitte and PwC. The main research question of the thesis is that what are the impacts and meanings of COVID-19 to the organizations' cyber security in the discourse produced by these two cyber security consulting firms. The thesis also analyzes what are the possible consequences and implications of this discourse for our understanding about the cyber security and what kind of power relations regarding cyber security are produced in the analyzed publications. The thesis is based on social constructionism's understanding of reality. Social constructionism sees the social realities as something that are constructed in human interactions, especially via the use of language. The applied research method in the thesis is the Habermasian discourse analysis. In the Habermasian discourse analysis the texts are analyzed using the validity claims of communication by Jürgen Habermas. Habermas has defined four validity claims which are truth, legitimacy, sincerity and comprehensibility. The key finding of the thesis is that in the publications of cyber security consulting firms the COVID-19 pandemic is seen as an unpredictable rupture which has increased the cyber risks for the organizations. To successfully operate in the midst of the pandemic, the organizations are advised to update their cyber security capabilities, both technology- and process-wise. It was also noticed that the publications produce and uphold the understanding where cyber security is seen as a domain of cyber security specialists and decision makers and where the employees and end-users are mainly seen as sources for cyber risks.

Keywords: cyber security, COVID-19, cyber security consulting, social constructionism, discourse analysis, Jürgen Habermas

KUVIOT

TAULUKOT

SISÄLLYS

1 JOHDANTO

> With the Covid-19 outbreak, cyber criminals have seized this global crisis to launch treacherous cyber exploits. The new normal landscape has generated a surge of sophisticated Gen V cyber attacks, including targeted ransomware. The Cyber Pandemic is here. (Check Point 2021).

Maaliskuun 11. päivä 2020 Maailman terveysjärjestö WHO julisti COVID-19-koronavirustaudin globaaliksi epidemiaksi eli pandemiaksi (WHO 2020). Pandemian myötä ihmisten liikkumista ja kokoontumista on rajoitettu useissa maissa ympäri maapalloa merkittävästi tämän kirjoitushetkellä jo yli vuoden ajan. Tällä on ollut useiden organisaatioiden päivittäiselle toiminnalle myös tuntuvaa vaikutusta, kun työntekijät ovat konttorille saapumiseen sijaan viranomaisten määräysten ja suositusten mukaisesti hoitaneet työtehtäviään kotoaan tai muusta etätyöskentelypisteestä käsin.

Pro gradu -tutkielmassani tutkin COVID-19-pandemian ympärille rakentuneita merkityksiä organisaatioiden kyberturvallisuuden kannalta. Kuten yllä olevasta tietoturvayhtiö Check Pointin sitaatista käy ilmi, on COVID-19-pandemian nähty lisänneen myös organisaatioihin kohdistuvia kyberriskejä. Tämän sanoman korostamiseksi kyseisessä sitaatissa käytetty kieli on hyvin kuvailevaa ja proosamaista, ja siitä löytyy ilmaisuja kuten ”sofistikoituneet hyökkäykset”, ”uusi normaali” ja ”kyberpandemia”. Pro gradu -tutkielmassani analyysini kohdistuu nimenomaan siihen kielenkäyttöön, jota tietoturvayhtiöt ovat COVID-19-pandemian vaikutuksista organisaatioiden tietoturvalle käyttäneet. Tämän kautta voimme paremmin ymmärtää sitä, miten kielenkäyttö vaikuttaa käsityksiimme kyberturvallisuudesta ja sen parantamiseksi tarvittavista toimenpiteistä.

1.1 Tutkimuskysymykset

Pro gradu -tutkielmassani tarkastelen kahden monikansallisen tietoturvakonsultointipalveluja tarjoavan yrityksen, Deloitten ja PwC:n, julkisesti heidän

kotisivuiltaan saatavilla olevia COVID-19-pandemiaa sekä kyberturvallisuutta käsitteleviä vuoden 2020 aikana ilmestyneitä julkaisuja, kuten artikkeleita, blogikirjoituksia ja raportteja. Tälle tutkimusaineistolle tutkielmassani esitetään seuraavat tutkimuskysymykset:

- Millaiseksi COVID-19-pandemian merkitys ja vaikutus organisaatioiden kyberturvallisuudelle tutkimusaineistossa kuvataan?
    - Millaisiin asiayhteyksiin COVID-19 aineistossa yhdistetään kyberturvallisuuden osalta?
    - Millaisia kyberturvallisuusuhkia ja -riskejä COVID-19-pandemiaan liitetään?
    - Millaisia toimenpidesuosituksia kyberturvallisuuden osalta COVID-19-pandemian keskellä toimimiseksi annetaan?
    - Mitä tekijöitä ja osa-alueita kyberturvallisuuden osalta COVID-19-pandemiaan liittyen aineistossa korostetaan? Tapahtuuko tämä mahdollisesti jonkun muun osa-alueen kustannuksella?
    - Mikä on tietoturvakonsultin rooli organisaatiolle COVID-19-pandemian keskellä?
- Mitä mahdollisia seurauksia ja vaikutuksia julkaisujen kielenkäytöllä on ymmärryksellemme kyberturvallisuudesta COVID-19-pandemian aikana?
- Millaisia kyberturvallisuuteen liittyviä valtasuhteita julkaisut tuottavat ja ylläpitävät?

Pro gradu -tutkielmani perustuu sosiaalisen konstruktionismin ymmärrykselle todellisuuden luonteesta sekä diskurssianalyyttiseen tutkimusmenetelmään. Sosiaalisessa konstruktionismissa todellisuuden ymmärretään rakentuvan ihmisten välisessä vuorovaikutuksessa. Keskeinen vuorovaikutuksen muoto on puolestaan kielenkäyttö, jota voidaan tutkia diskurssianalyysin keinoin. Diskurssianalyysissa keskiössä on sen tutkiminen, millaisia merkityksiä tutkittavasta aiheesta tutkimusaineiston käyttämä kieli tuottaa, ja miten se siten rakentaa sosiaalista todellisuutta tämän aiheen ympärille. Keskeinen käsite diskurssianalyyttisessa tutkimuksessa on valta, eli se kenen asiaa ja etuoikeuksia käytetty kieli ajaa, ja kenen ääni puolestaan jää kuulumattomiin.

Pro gradu -tutkielmani tutkimusaiheen kontekstissa tämä tarkoittaa sitä, että analysoitavat tietoturvakonsultointyhtiöiden julkaisut osaltaan tuottavat ja rakentavat ymmärrystämme todellisuudesta koskien COVID-19-pandemian merkitystä organisaatioiden kyberturvallisuudelle ja tutkielman tutkimuskysymyksiin vastaamalla voimme tätä rakennusprosessia ymmärtää ja avata. Työkaluna tämän rakennusprosessin avaamisessa toimii puolestaan diskurssianalyysi. Tutkielmassani käytettävää diskurssianalyyttista menetelmää voidaan kutsua habermasilaiseksi diskurssianalyysiksi (ks. Cukier 2004 & 2009). Habermasilaisessa diskurssianalyysissa tutkimusaineistoa tarkastellaan Jürgen Habermasin neljän kommunikaation pätevyysvaatimuksen kautta, jotka ovat totuus, oikeellisuus, vilpittömyys ja ymmärrettävyys (Edgar 2005, 148-149). Totuuden osalta tarkastellaan aineistosta löytyviä totuusväittämiä ja niiden perusteita,

oikeellisuuden kohdalla ollaan kiinnostuneita asioista, jotka korostuvat aineistossa ja siitä, kenen ääni aineistossa on kuuluvilla. Vilpittömyyden osalta analysoidaan teksteistä löytyviä kuvailevia ilmauksia sekä konnotaatioita ja ymmärrettävyyden pohjalta tarkastellaan ylipäätään tekstin ymmärrettävyyttä lukijalle ja ymmärrettävyyttä mahdollisesti heikentävien epäselvien termien, kuten esimerkiksi teknisen jargonin käyttöä. Tässä tutkielmassa käytetty teoreettinen ja metodologinen kehys tullaan tarkemmin avaamaan tutkielman luvuissa 2 ja 3.

1.2 Tutkimusaiheen valinnan ja rajauksen perusteet

Pro gradu -tutkielmani tutkimusaiheen valinnalle on sekä akateemisia että pragmaattisia perusteita. Akateemisten perusteiden osalta aiheena oleva tietoturvakonsultointiyhtiöiden COVID-19-diskurssin tutkiminen on tärkeää, koska se kiinnittää huomion myös kyberturvallisuutta koskevaan konstruktionistiseen puoleen, jossa uhkien, riskien ja turvallisuuden ymmärretään rakentuvan osittain myös kielenkäytön kautta. Tällainen suhtautuminen turvallisuuden tutkimukseen on informaatioteknologian puolella toistaiseksi ollut vähäistä, enkä esimerkiksi Jyväskylän yliopistossa kyberturvallisuuden maisteriohjelmassa ole törmännyt siihen kertaakaan. Syynä tähän on mahdollisesti tieteenalan matemaattis-luonnontieteellinen tausta ja pohjavire, jossa konstruktionismin sijaan vallalla on ollut positivistisempi lähestymistapa tutkimuskohteisiin ja -kysymyksiin sekä pyrkimys selkeiden syy-seuraussuhteiden tunnistamiseen ilmiöiden ja niihin sisältyvien merkitysten kuvailun ja tulkinnan sijaan.

COVID-19-pandemian kaltainen tilanne on diskurssianalyyttiselle tutkimukselle hedelmällinen johtuen sekä sen ajankohtaisuudesta että pandemian saamasta laajasta huomiosta läpi yhteiskunnan eri sidosryhmien. Tietoturvayhtiöiden julkaisuja on kyberturvallisuuden tutkimuksessa käytetty perinteisesti tutkimuskirjallisuuden omaisesti, mutta tutkielmassani nämä muodostavat analysoitavan kohteen. Tämä puolestaan pohjautuu diskurssianalyyttisen tutkimuksen keskuudessa vallitsevalle ymmärrykselle, jossa tieteellistä tutkimusta, mukaan lukien diskurssianalyyttista, ja asiantuntijalausuntoja pidetään yhtä lailla merkityksiä ja sosiaalista todellisuutta rakentavina tuotoksina ja siten myös itsessään diskurssianalyysin kohteina (Juhila 2002, 230).

Deloitte ja PwC valikoituivat analysoitaviksi tietoturvayhtiöiksi sen takia, että nämä kaksi yhtiötä on nostettu tutkimuslaitos Forresterin (2019) *The Forrester Wave : Global Cybersecurity Consulting Services 2019 Q2* -raportissa kahdeksi johtavimmaksi globaaliksi tietoturvayhtiöksi. Täten heidän näkemyksillään ja kannanotoillaan kyberturvallisuudesta voidaan väittää olevan alan parissa tuntuvaa painoarvoa. Tutkielman suunnitteluvaiheessa tarkoituksena oli ottaa mukaan suurempi joukko tietoturvayhtiöitä, mutta työn laajuus ja käytetty tutkimusmenetelmä huomioiden tämä ei ollut mahdollista.

Pragmaattisten syiden osalta tutkimusaiheen valintaan vaikuttivat sekä koulutustaustani että työtehtäväni tutkielman kirjoitushetkellä. Olen aiemmalta

koulutukseltani valtiotieteiden maisteri ja pääaineessani valtio-opissa ja sen kansainvälisten suhteiden tutkimuksen suuntauksessa konstruktionistinen turvallisuudentutkimus on ollut hyvin suosittu tutkimussuuntaus. Sen takia halusin hyödyntää tätä entuudestaan tuntemaani teoria- ja menetelmäpohjaa myös kyberturvallisuuden maisteriohjelmaan tekemässäni pro gradu -tutkielmassa. Tutkielma on tehty opintovapaani aikana tammi-huhtikuussa 2021. Työn aloitusajan takia rajasin vuotta 2020 uudemmat julkaisut analysoitavan aineiston ulkopuolelle. Tutkielman kirjoitushetkellä työskentelen tietoturvakonsulttina yhtiössä, jota voidaan pitää tutkimusaineistona olevien Deloitten ja PwC:n merkittävänä kilpailijana. Tämä yksityiskohta on mielestäni tärkeää tuoda esiin, mutta tutkielmani tarkoituksena ei ole työnantajani kilpailijoiden kritisoiminen tai mustamaalaaminen, vaan samankaltaisia havaintoja, joita työn analyysiluvuissa tulee ilmi, on löydettävissä yhtä lailla oman työnantajayhtiöni samaa aihealuetta koskevista julkaisuista.

1.3 Tutkielman rakenne

Tutkielmani koostuu kahdeksasta pääluvusta. Johdannon, eli työn ensimmäisen luvun, jälkeen avaan toisessa luvussa tarkemmin sosiaalista konstruktionismia, joka toimii tutkielman teoreettisena viitekehyksenä. Samassa luvussa tarkastelen myös sosiaalisen konstruktionismin hyödyntämistä turvallisuudentutkimuksessa. Luvussa 3 puolestaan käydään läpi työn tutkimusmenetelmä eli habermasilainen diskurssianalyysi. Habermasilaisen diskurssianalyysin ymmärtämiksi avaan luvussa tarkemmin myös diskurssianalyyttisen tutkimuksen pääsuuntauksia sekä lyhyesti lisäksi Jürgen Habermasin kommunikatiivisen toiminnan teoriaa. Luvussa 4 esittelen tarkemmin tutkimusaineistona toimivia Deloitten ja PwC:n julkaisuja. Luvut 5, 6 ja 7 ovat tutkielman varsinaisia aineiston analyysia koskevia lukuja. Luvussa 5 aineistoa tarkastellaan totuuden pätevyysvaatimuksen kautta, luvussa 6 oikeellisuuden pätevyysvaatimuksen kautta ja luvussa 7 sekä vilpittömyyden että ymmärrettävyyden pätevyysvaatimusten kautta. Luku 8 on tulos- ja johtopäätösluku, jossa kerrataan tutkielman keskeiset havainnot, pohditaan näiden seurauksia ja merkitystä sekä mietitään mahdollisia näiden havaintojen kannustamia lisätutkimuskohteita.

Kyberturvallisuuden ja tietoturvallisuuden käsitteiden sisältämistä merkityseroista on käyty myös akateemista keskustelua (ks. esim. Bay 2016), mutta tutkielmassani en lähde tähän keskusteluun mukaan, vaan käytän näitä käsitteitä rinnasteisesti toistensa synonyymeina läpi työn.

2 SOSIAALINEN KONSTRUKTIONISMI – TUTKIELMAN TEOREETTINEN VIITEKEHYS

Tässä luvussa avaan pro gradu -tutkielmani teoreettisia lähtökohtia. Luku alkaa tutkielmani teoriakehyksenä toimivan sosiaalisen konstruktionismin yleisesittelyllä. Tämän jälkeen käyn tarkemmin läpi esimerkkejä sosiaaliseen konstruktionismiin pohjautuvista turvallisuudentutkimuksen suuntauksista, tarkemmin ottaen kriittisestä turvallisuudentutkimuksesta. Lisäksi luvussa selvennän sosiaalisen konstruktionismin merkitystä ja suhdetta oman tutkimusaiheeni, eli tietoturvakonsultointiyhtiöiden COVID-19-diskurssin kannalta.

2.1 Sosiaalisen konstruktionismin lähtökohdat

Pro gradu -tutkielmani tieteenfilosofisena ja tutkimuksellisena teoriakehyksenä toimii sosiaalinen konstruktionismi. Sosiaalisen konstruktionismin perusajatuksena on todellisuuden rakentuminen ihmisten välisessä vuorovaikutuksessa ja kielenkäytössä. Tämän perusajatuksen Berger & Luckmann (1994) ovat kiteyttäneet teoksessaan *Todellisuuden sosiaalinen* rakentuminen. Sosiaalista konstruktionismia voidaan pitää vastakohtana positivismille ja essentialismille, joiden lähtöoletuksena on mahdollisuus objektiivisesti havainnoida ja kerätä tietoa ympäristössämme olevien asioiden perusluonteesta tai -olemuksesta. (Burr 2003, 3 & 5 ; Lock & Strong 2011, 7).

Sosiaalisessa konstruktionismissa ei ole kyse yhdestä yhtenäisestä oppisuuntauksesta, mutta sille on tunnistettavissa tiettyjä yhteisiä nimittäjiä (Burr 2003, 2 ; Lock & Strong 2011, 6). Lock & Strong (2011, 6-7) ovat nähneet sosiaalisen konstruktionismin keskiössä olevan merkityksen ja ymmärryksen tutkimisen ihmisten välisestä kanssakäymisestä, jotta voitaisiin esimerkiksi ymmärtää miten eri kieltä puhuvien ihmisten kokemukset eroavat toisistaan verrattuna samaa kieltä puhuviin.

Burr (2003, 2) on puolestaan esittänyt sosiaalisen konstruktionismin perustuvan neljään ydinolettamukseen, joista sosiaaliseksi konstruktionismiksi määriteltävä tutkimus nojaa vähintään yhteen, mutta mahdollisesti useampaan tai näihin kaikkiin. Ensimmäisenä perusolettamuksena on nimenomaan jo edellä mainittu vastakohtainen asennoituminen positivismin käsitykseen todellisuudesta (Burr 2003, 2-3). Siinä missä positivisti seistessään talon edessä voisi olla kiinnostunut siitä, mistä materiaaleista talo on rakennettu, millä värillä se on maalattu ja kuinka monta naulaa siihen on käytetty, voisi sosiaalinen konstruktionisti puolestaan olla kiinnostunut siitä, mitä merkityksiä talon rakentajat ja siellä asuvat ovat esimerkiksi näihin materiaalivalintoihin tai rakennuksen muotoihin liittäneet. Tietoturvan kontekstissa positivistinen tutkija saattaisi olla kiinnostunut siitä, mitä eri tietoturvarooleja organisaatiossa on ja miksi. Sosiaalisen konstruktionistin tutkimuskysymyksenä saattaisi puolestaan olla se, mitä näissä eri rooleissa toimivat henkilöt ymmärtävät ylipäätään tietoturvalla tarkoitettavan ja miten se puolestaan vaikuttaa siihen, miten he tehtäviään hoitavat. Esimerkit ovat toki kärjistettyjä, mutta niiden kautta voidaan hahmottaa näiden kahden suuntauksen välistä eroa ajattelussa.

Burr (2003) jatkaa, että sosiaalisessa konstruktionismissa tärkeää on pyrkimys suhtautua kaikkeen tietoon ja ymmärrykseen maailmasta kriittisesti. Sosiaalisen konstruktionismin lasien läpi tarkasteltuna kategoriat ja luokittelut, joilla maailmaa jäsennämme, eivät näyttäydy absoluuttisina totuuksina ympäröivästä maailmastamme, vaan ne ovat aina tulkinnanvaraisia ja muutoksessa olevia. (Burr 2003, 2-3). Esimerkiksi mikä tekee kansallisvaltiosta kansallisvaltion? Onko se mahdollisesti lippu, maantieteelliset rajat tai tällä maantieteellisellä alueella asuvien ihmisten etninen tausta? Vai onko kyse ennemminkin yhteisesti jaetuista uskomuksista, ideoista ja symboleista, joiden kautta ymmärrys kansallisvaltiosta määrittyy (ks. Anderson 2006)? Vastaavaa todellisuuden määrittelyn problematiikkaa löytyy ympäriltämme kaikesta, kuten sukupuolesta (ks. esim. Butler 2006), rahasta (ks. esim. Deutschmann 1996) sekä myös turvallisuudesta. Turvallisuuden ja kyberturvallisuuden konstruoinnin osalta palaan sen problematiikkaan seuraavassa alaluvussa tarkemmin.

Toinen sosiaalisen konstruktionismin ydinolettamus koskee ymmärryksemme todellisuudesta kiinteää nivoutumista historialliseen ja kulttuuriseen kontekstiin ja ajanhetkeen. Ymmärryksemme ja tulkintamme ympäröivästä todellisuudesta muotoutuu aina sen kautta, millaisissa olosuhteissa ja kontekstissa elämme ja tuota ymmärrystä muodostamme. (Burr 2003, 3-4). Esimerkiksi Jyväskylän yliopistolla kyberturvallisuuden maisteriohjelmassa olevien opiskelijoiden ymmärrys ja tulkinta yliopistosta instituutiona tai sodankäynnistä käsitteenä, on varmasti hyvin erilainen mitä se oli vaikkapa Turun Akatemian teineillä 1600-luvun lopulla tai Eurooppaan 1200-luvulla saapuneilla mongolijoukoilla. Eikä esimerkkejä tarvitse hakea edes näin kaukaa. Todennäköistä on, että näitä käsitteitä koskevia ymmärrys- ja tulkintaeroja löytyy myös saman oppiaineen opiskelijoiden sisältä.

Kolmantena ydinolettamuksena on, että ymmärryksemme todellisuudesta rakentuu sosiaalisissa prosesseissa. Siinä missä positivistit pyrkivät

havainnoimalla saamaan irti tietota todellisuuden perusolemuksesta, sosiaaliset konstruktionistit näkevät tiedon ja todellisuuden rakentuvan ihmisten välisessä kanssakäymisessä. Tässä kanssakäymisessä kielellä on keskeisin merkitys ja siksi sosiaalisen konstruktionismiin perustuva tutkimus tutkii ja analysoi ihmisten välisiä merkitysjärjestelmiä, joista ensisijaisena on puhuttu ja kirjoitettu kieli. Ihmisten puhuessa tai muuten kommunikoidessa toisilleen, he samalla rakentavat sosiaalista todellisuutta. Tähän liittyy *performaation* käsite, jolla tiivistetysti tarkoitetaan sitä, puheella ja kielellä on käytännön seurauksia, esimerkiksi papin julistaessa avioparin mieheksi ja vaimoksi, valtion päämiehen julistaessa sodan toiselle valtiolle tai tietoturva-auditoijan julistaessa asiakasorganisaation tietojärjestelmän hyväksytysti tietoturvasertifioiduksi. (Burr 2003, 4-5 & 7).

Neljäntenä ja viimeisenä ydinolettamuksena sosiaalisessa konstruktionismissa ymmärryksemme ja tietomme todellisuudesta nähdään kulkevan käsi kädessä sosiaalisen toiminnan kanssa. Eli kuten edellä mainitussa performaatioesimerkissä kävi ilmi, valitulla puheella ja kielellä on vaikutusta siihen, millaiseksi ympäröivä todellisuutemme muodostuu ja mitä konkreettisesti meihin vaikuttavia asioita siellä tapahtuu. Sosiaalisessa konstruktionismissa tieto ei ole siten jotain sellaista, mitä meillä on tai ei ole, vaan sosiaalisen konstruktionismin kehyksessä tieto ja siitä koituvat seuraukset syntyvät ihmisten välisessä vuorovaikutuksessa. (Burr 2003, 5 & 9). Avartava ja laajasti tutkittu esimerkki käytetyn kielen voimasta ja vaikutuksesta arkitodellisuuteen turvallisuuden kontekstissa on George W. Bushin hallinnon terrorismin vastaisen sodan retoriikka (esim. Hodges 2011 ; Jackson 2005 ; Rantapelkonen 2006). Tällä retoriikalla rakennettiin ja tuotettiin ymmärrys vuoden 2001 terrori-iskuista nimenomaan sodanjulistuksena Yhdysvaltoja vastaan. Tässä ymmärryksessä ja diskurssissa Yhdysvaltojen tuli myös vastata näihin iskuihin sotatoimin sen sijaan, että iskuista olisi puhuttu esimerkiksi rikoksena, johon vastaus olisi ollut ensisijassa poliisioperaatiot sotilaskoneiston palvelukseen valjastamisen sijasta.

Pro gradu -tutkielmani osalta tukeudun kaikkiin neljään Burrin nimeämään sosiaalisen konstruktionismin ydinolettamukseen. Tulkinnassani käsitteet kuten turvallisuus, kyber, uhka ja riski eivät ole kiveen hakattuja yhden totuuden käsitteitä, vaan näiden merkitys ja tietosisältö rakentuvat uudelleen ja uudelleen vuorovaikutuksessa ja kommunikaatiossa, jota käydään alan asiantuntijoiden, päättäjien, akateemisen tutkimuksen, median ja niin sanottujen tavallisten kansalaisten välillä. Tämä vuorovaikutus on aina myös sidoksissa ympäröivään historialliseen, kulttuuriseen ja yhteiskunnalliseen kontekstiinsa, eikä sen merkitystä voi analyysissa sivuuttaa. Tietoturvayhtiöiden COVID-19-diskurssin ja sen sosiaalisen rakentumisen analyysin tärkeys nousee siitä, että sosiaalisen konstruktionismin kehyksessä valitulla kielenkäytöllä on keskeinen merkitys sille, millaisia käytännön toimia ja tekoja vallalla olevasta kielenkäytöstä nousee. Koetaanko COVID-19 kyberturvallisuuden kannalta esimerkiksi vain väliaikaisen katkoksena vai perustellaanko sillä koko ajan kiristyvien turvallisuustoimien tarvetta myös COVID-19-pandemian päättymisen jälkeen niin sanotussa "uudessa normaalissa"?

2.2 Turvallisuuden ja kyberturvallisuuden sosiaalinen rakentuminen

Turvallisuuden tutkimuksessa huomio on usein ollut siinä, mitä halutaan turvata ja millä keinoin sen sijaan, että siinä problematisoitaisiin turvallisuuden käsitettä itsessään (Vuori 2011, 94). Sosiaaliseen konstruktionismiin perustuvissa tutkimussuuntauksissa tätä painotusta on pyritty haastamaan ja siirtämään fokus siihen, miten turvallisuutta, sen sukulaiskäsitteitä ja näiden merkityssisältöjä ihmisten välisessä vuorovaikutuksessa tuotetaan ja rakennetaan, ja mitä seurauksia näistä merkityksenannoista puolestaan seuraa. Esimerkiksi Campbell (1998) on esittänyt, että vaara ei ole objektiivinen tila tai olosuhde. Tekemällä rajanvetoa siitä, mikä kuuluu sisäpuolelle ja mikä puolestaan on uhkaavaa ja tulee jättää ulos, on keskeinen merkitys valtioiden määritellessä omaa identiteettiään ja olemassaolonsa tarkoitusta. (Campbell 1998, 1-3 & 9).

Myös sillä on merkitystä mitä asioita koemme turvallisiksi ja mitä puolestaan emme, ja kuinka turvallisina turvallisiksi mieltämiämme asioita pidämme. Esimerkiksi jostakin tietojärjestelmästä tehty tietoturvatarkastusraportti muokkaa ymmärrystämme ja mielikuvaamme siitä, kuinka turvallinen tämä järjestelmä on. Käsityksellä järjestelmän turvallisuudesta tai turvattomuudesta puolestaan voi olla vaikutusta siihen, kuinka halukkaita ja kiinnostuneita tällaista järjestelmää vastaan ollaan hyökkäämään. (Pieters 2011, 333).

Riskin käsitteen kohdalla sitä koskevien merkitysten ja ymmärryksen painoarvoa ei voi myöskään ohittaa. Riskejä ja niiden suuruuksia kuvataan usein luonnontieteellisyyttä korostavina matemaattisina kaavoina, kuten *Riski = Todennäköisyys x Vaikutus*, vaikka se, mitä nostetaan riskeiksi ja mitä puolestaan ei, on vahvasti sidoksissa ympäröivään sosiaaliseen ja kulttuuriseen kontekstiinsa. (Stankiewicz 2008, 61-62). Yksilönvapautta korostavissa kulttuureissa on henkilötietojen oikeanlaiselle ja luottamukselliselle käsittelylle laitettu suuri painoarvo esimerkiksi rahallisesti sanktioimalla tietosuojarikkeistä. Totalitaarisessa kontekstissa puutteet yksittäisten kansalaisten henkilötietojen salassapidossa tuskin koettaisiin yhtä merkittäväksi riskiksi, pahimmillaan mahdollisesti jopa tavoiteltavaksi asiantilaksi. Riskiarvioissa näkyvillä numeerisilla arvoilla voidaan pyrkiä vaikuttamaan ja perustelemaan esimerkiksi riskejä kontrolloivien investointien tarpeellisuutta (ks. esim. Wang et al. 2008). Riskiarvioinneissa esimerkiksi töidensä puolesta mukana olleet kuitenkin tietävät, että näiden numeroiden taakse lähes aina paljon myös subjektiivisia mielipiteitä ja agendoja, kun eri sidosryhmät haluavat saada numerot näyttäytymään itsensä kannalta suotuisilta. Toisin sanoen yksinomaan kylmän matemaattisuuden sijaan myös nämä numerot muotoutuvat sosiaalisessa vuorovaikutuksessa.

2.2.1 Kriittinen turvallisuudentutkimus

Sosiaaliseen konstruktionismiin nojaava ja siitä vaikutteita ottanut turvallisuudentutkimus on ollut viime vuosikymmeninä suosiotaan kasvattava

lähestymistapa erityisesti kansainvälisten suhteiden tutkimuksessa, jonka parista on tehty tätä lähestymistapaa hyödyntävää tutkimusta myös kyberturvallisuutta koskevien kysymysten osalta (ks. esim. Hansen & Nissenbaum 2009 ; Lacy & Prince 2018 ; Liebetrau & Christensen 2021) . Yksi näistä sosiaaliseen konstruktionismiin perustuvista tutkimussuuntauksista on niin sanottu *kriittinen turvallisuudentutkimus*. Kriittinen turvallisuudentutkimus toimii kattoterminä turvallisuudentutkimusta sekä marxilaisvaikutteista kriittistä teoriaa yhdistävälle tutkimukselle, mutta kyseessä ei ole yksi yhtenäinen tutkimussuuntauksensa. Tärkeinä kriittisen turvallisuudentutkimuksen yhteisinä nimittäjinä toimivat huomion suuntaaminen perinteisiä turvallisuuden tutkimuskohteita eli valtioita ja sotilaallista turvallisuutta laajemmin myös muihin turvallisuuden osa-alueisiin, kuten ympäristöön, talouteen, ihmisiin, mutta myös kyberturvallisuuteen, sekä diskurssien merkitykseen turvallisuutta koskevan ymmärryksemme rakentumisessa. (Peoples & Vaughan-Williams 2010, 3-6 & 18). Luen pro gradu -tutkielmani kuuluvaksi osaksi kriittisen turvallisuudentutkimuksen traditiota, koska tutkimuskohteenani on kyberturvallisuuden diskurssi COVID-19-pandemian kontekstissa ja tästä diskurssista mahdollisesti aiheutuvat seuraukset niin yksilöiden kuin organisaatioidenkin kyberturvallisuudelle.

Kriittisen turvallisuudentutkimuksen nimessä oleva "kriittisyyden" käsite on saanut osakseen myös oman kritiikkinsä. Suuntauksen saavuttama suosio ja sisäinen monimuotoisuus ovat esimerkiksi Hynekin & Chandlerin (2013) mukaan syitä, miksi kriittisyys sanana olisi perusteltua tiputtaa tutkimussuuntauksen nimestä pois. Toiseksi tutkimussuuntauksen alkuperäinen emansipatorinen luonne, toisin sanoen länsimaailman interventionistisen ulkopolitiikan kritiikki ja radikaalien vaihtoehtojen esittäminen, on heidän mielestään pudonnut pois tai ainakin muuttanut muotoaan niin paljon, että perusteita tutkimussunnauksen kutsumiseksi kriittiseksi ei enää ole. (Hynek & Chandler 2013, 46-48). Toisaalta Peoples & Vaughan-Williams (2010, 1) ovat osuvasti todenneet, että olisi vaikea kuvitella turvallisuudentutkimuksen suuntausta, joka olisi "epäkriittinen". Tämän enempää en pro gradu -tutkielmassani kuitenkaan lähde mukaan tutkimussuuntauksen oikeanlaista nimeä koskevaan semanttiseen pohdintaan, vaan ehkä yksinkertaistamisenkin riskin nojalla kutsun edustamaani tutkimussuuntausta yleisten konventioiden mukaisesti edelleen turvallisuudentutkimuksen kriittiseen traditioon lukeutuvaksi.

2.2.2 Case turvallistamisteoria & teorian hyödyntäminen kyberturvallisuuden tutkimuksessa

Ymmärtääksemme kattavammin sosiaalisen konstruktionismin lähtökohtien hyödyntämistä turvallisuudentutkimuksessa, avaan esimerkinomaisesti tarkemmin todennäköisesti eniten huomiota saanutta kriittisen turvallisuudentutkimuksen alasuuntausta. Tämä suuntaus on niin sanotun Kööpenhaminan

koulukunnan tunnetuksi tekemä turvallistamisteoria, jossa keskiössä on se, miten turvallisuus on ennen kaikkea puheen kautta tapahtuvaa tekemistä (Vuori 2011, 103). En omassa pro gradu -tutkielmassani hyödynnä turvallistamisteoriaa kokonaisuudessaan, mutta nostan analyysiosiossa tästä huolimatta esiin turvallistamisretoriikalle tunnusomaisia esimerkkejä, vaikka en tulekaan ottamaan kantaa siihen, onko tämä turvallistaminen laajemmassa yhteiskunnallisessa kontekstissa onnistunut vai ei. Lisäksi kyseisen teorian avaaminen tässä yhteydessä on hyödyllistä, sillä teoria jakaa samat premissit kielenkäytön roolista turvallisuuden rakentumisessa kuin oma pro gradu -tutkielmani.

Turvallistamisteorian perusteet esitteli Barry Buzanin, Ole Wæverin sekä Jaap de Wilden vuonna 1998 julkaistu teos *Security: A New Framework for Analysis*. Buzanin, Wæverin ja de Wilden mukaan heidän kirjansa päätarkoitus oli esittää teoriakehys, jossa turvallisuutta ei rajattaisi koskemaan ainoastaan sotilaallisia kysymyksiä, sillä kyseinen perinteisen turvallisuudentutkimuksen näkemys turvallisuudesta on liian kapea. Heidän mielestään turvallisuuden keskiössä on se, miten jokin asia, sotilaallinen tai ei-sotilaallinen, nousee tavallisesta poliittisesta keskustelusta turvallisuuskysymykseksi. Jotta tämä voi onnistua, on turvallistavan toimijan muodostettava asiasta tietyn viitekohteen olemassaoloa uhkaava eksistentiaalinen uhka, joka edellyttää poikkeuksellisia hätätoimenpiteitä, joita muuten ei hyväksyttäisi tai jotka muuten olisivat olemassa olevan lainsäädännön vastaisia. (Buzan et al. 1998, 4-5).

Turvallistamisteoriassa olemassaoloa uhkaava eksistentiaalinen uhka ei rajoitu ainoastaan valtioiden selviytymistä ja olemassaoloa uhkaaviin tekijöihin, vaan eksistentiaalinen uhka voi tarkoittaa esimerkiksi jonkin poliittisen ideologian selviytymistä, organisaation liiketoiminnan jatkumista, etnisen yhtenäisyyden tai jonkin tietyn lajin tai koko ilmaston säilymistä uhkaavaa tekijää (Buzan et al. 1998, 21-23). Turvallistamisen onnistumiseksi eksistentiaalinen uhka ei riitä yksinään, vaan tämä pitää saada teorian nimen mukaisesti turvallistettua. Buzan et al. (1998, 23-24) jakavat julkiset asiat ja kysymykset kolmeen luokkaan:

1. Politisoimattomat asiat, jotka eivät ole julkisen keskustelun tai päätöksenteon piirissä.
2. Politisoidut asiat, jotka ovat mukana keskustelussa ja joiden hoitamiseksi tehdään päätöksiä ja allokoidaan resursseja.
3. Turvallistetut asiat, jotka näyttäytyvät eksistentiaalisena uhkana, edellyttävät poikkeuksellisia keinoja ja toimenpiteitä, jotka eivät politisoitujen asioiden kohdalla olisi vielä mahdollisia.

Buzan et al. (1998, 24) mukaan rajanveto politisoidun ja turvallistetun kysymyksen välille on keskeisiä haasteita turvallisuuden tutkimuksessa.

Turvallistamisteoriassa kielenkäytöllä on keskeinen rooli, sillä tietty politisoitu kysymys turvallistetaan nimenomaan eksistentiaalisen uhan retoriikalla. Turvallistamisen onnistumiseksi tarvitaan turvallistavan retoriikan lisäksi yleisön tuki ja hyväksyntä tälle retoriikalle ja diskurssille. Yleisön hyväksynnän kautta voidaan oikeuttaa normaaleja politiikan sääntöjä rikkovat erityistoimenpiteet. Näin ollen onnistunut turvallistaminen koostuu kolmesta osatekijästä:

eksistentiaalisesta uhasta, poikkeuksellisista hätätoimenpiteistä sekä sääntöjen rikkoutumisesta ja niistä irtautumisesta. (Buzan et al. 1998, 24-26).

Turvallistamisteorian kehyksessä kielenkäyttö ymmärretään puheaktina, jossa jotakin sanomalla itse asiassa tehdään tämä jokin (Buzan et al. 1998, 26). Teorian taustalla olevassa J.L Austinin puheaktiteoriassa puheaktit jaetaan kolmeen ryhmään: lokuutiolla tarkoitetaan puheen lausumisen fyysistä tekoa, illokuutiolla lausumalla tapahtuvaa tekoa ja perlokuutiolla tekoa, jolla puhuja saa lausuessaan yleisössä aikaan jonkin vaikutuksen. Turvallistamisen keskiössä ovat illokutionaariset puheaktit, eli lausumalla jotakin, jotakin myös tapahtuu. Turvallistamisteorian kontekstissa illokutionaarisella puheaktilla jokin tietty kysymys (esim. tiedustelulainsäädännön päivittämättä jättäminen) pyritään tuottamaan olemassaolon uhkana jollekin viitekohteelle (esim. kansallinen turvallisuus). (Vuori 2004, 5-6). Illokutionaariset performatiiviset puheaktit, eli aktit joissa jotakin lausumalla myös tehdään jotakin, ovat keskeisiä todellisuuden rakennuspalikoita sosiaalisen konstruktionismin näkökulmasta ja osoitus siitä, miten kielenkäyttömme rakentaa ymmärrystämme todellisuudesta.

Turvallistamisen onnistuessa mahdollistetaan normaaleista politiikan säännöistä poikkeaminen ja näiden ohittaminen (esim. lain vieminen kiireellisenä poikkeusjärjestelyin eteenpäin) nostamalla turvallistettu kysymys ”erityispolitiikan areenalle” (Vuori 2004, 5-6). Läntisessä maailmassa turvallistaminen ja sen muodostama eksistentiaalinen uhka toisin sanoen mahdollistaa toimet, jotka muuten eivät olisi hyväksyttyjä vapaassa ja demokraattisessa yhteiskunnassa. Täten turvallistamisteorian pohja löytyy saksalaisen yhteiskuntateoreetikon Carl Schmittin ajattelusta koskien poikkeustilaa, jossa suvereeni toimija, eli valtio, voi määrittämällään poikkeustilan irtautua laeista ja säädöksistä suojellakseen suvereniteetin säilymistä. (Poutanen 2016).

Turvallistamisteoriaa on sovellettu myös kyberturvallisuuden tutkimisessa. Hansen & Nissenbaum (2009) ovat tunnistaneet kyberturvallisuuden diskurssista tietoverkkoturvallisuuden ja yksilöiden turvallisuuden olemassaololtaan uhatuiksi viitekohteiksi, jotka kuitenkin linkittyvät laajemmassa kuvassa valtion, yhteiskunnan, kansan ja talouden viitekohteisiin. Kyseiset viitekohteet ovat Hansenin & Nissenbaumin mukaan turvallistettu kolmella eri tavalla: 1) yliturvallistamisella (*hypersecuritization*), joka nojautuu kyberkatastrofien varaan, 2) jokapäiväisillä turvallisuuskäytännöillä, joilla pyritään turvallistamaan kansalaisten arkielämä sekä 3) teknillistämällä (*technification*), jolla kyberturvallisuudesta tehdään teknistä erityisosaamista omaavien eksperttien toimintakenttää.

Kehittämäänsä viitekehystä Hansen & Nissenbaum ovat soveltaneet tutkimuksessaan Viron kevään 2007 tapahtumiin, jolloin Viron viranomaisten toimesta toisessa maailmasodassa kaatuneita neuvostosotilaita muistanut pronssipatsas siirrettiin Tallinnan keskustasta kauemmas hautausmaalle aiheuttaen sekä mielenosoituksia että Viron viranomaisten ja yksityisten tahojen hallinnoimiin palveluihin kohdistuneita palvelunestohyökkäyksiä. Hansen & Nissenbaum (2009, 1168-1169) pitävät näitä tapahtumia seurannutta Viron viranomaisten diskurssia esimerkkinä vähintäänkin osittain onnistuneen kyberturvallisuuden turvallistamisena, sillä hyökkäyksistä muodostui ja vakiintui kielenkäytön

kautta ymmärrys ”ensimmäisestä sodasta kyberavaruudessa”, jossa esimerkiksi pankkipalvelut, viranomaisten kanssa asiointi ja uutissivustojen lukeminen linkittyivät osaksi ”yksilöllistä turvallisuutta” ja jossa DDoS-hyökkäykset tulkittiin Viron itsemääräämisoikeutta uhkaaviksi toimiksi.

Hansenin & Nissenbaumin ajatuksia kyberturvallisuuden diskursseista ovat jalostaneet Lacy & Prince (2018), jotka ovat tunnistaneet kolme ymmärrystämme kyberturvallisuudesta ja kybersodasta muovaavaa positiota ja diskurssia: 1) kyberkatastrofisti, jonka tulevaisuuden näkymät ja tuomiopäivän profetiat rakentuvat digitaalisten katastrofien varaan, 2) digitaalinen realisti, joka argumentoi ja pyrkii jarruttelemaan katastrofistin esittämiä näkemyksiä vastaan ja jolle kyberturvallisuuden uhat näyttäytyvät ennemminkin vähäisenä kiusana, mitkä eivät pärjää teknologiasta saataville hyödyille, sekä 3) tekno-optimisti, jolle historia on jatkuvaa kehitystä, missä teknologiaa voidaan hyödyntää katastrofiskenaarioissa esitettyjen uhkakuvien ennaltaehkäisemiseen.

Vaikka pro gradu -tutkielmassani en turvallistamisteoriaa sellaisenaan suoraan hyödynnäkään, ovat edellä kuvatut kyberturvallisuutta koskevat tunnistetut puhujapositiot sekä diskurssit hyvä pitää mielessä tutkielmani analyysiosioiden kohdalla, sillä vastaavan kaltaisia esimerkkejä tietoturvauhkien konstruoinnista tai diskurssin teknillistämisestä on löydettävissä myös tutkimusaineistonani käyttämistä tietoturvakonsultointiyhtiöiden COVID-19-aiheisista julkaisuista.

2.2.3 Kyberturvallisuudentutkimuksen erityispiirteet

Liebetrau & Christensen (2021) ovat kritisoineet kriittisen turvallisuudentutkimuksen ja erityisesti turvallistamisteorian valtiokeskeisyyttä kyberturvallisuuden tutkimuksessa. Heidän mukaansa valtioihin keskittyminen ei riitä ymmärtämään kyberturvallisuuden toimintadynamiikkaa, koska valtioiden lisäksi kyberturvallisuuteen kytkeytyy myös useita muita toimijoita ja tiloja. Lisäksi automatiikka ja robotiikka sekä ei-ihmistoimijat, kuten esimerkkinä bottiverkot, tuovat tutkimuskohteelle omat erityispiirteensä, joita ei voi redusoida kansallisvaltioiden turvallistamisretoriikkaan, jolle teknologia on aiemmassa tutkimuksessa jäänyt alisteiseksi. (Liebetrau & Christensen 2021, 26-28). Lisäksi Christensenin & Liebetraun (2009) mukaan kyberuhat ja -riskit eivät välitä valtioiden rajoista (ellei haittaohjelmiin ole esimerkiksi tekijänsä toimesta asetettu näitä huomioivia valtiokohtaisia IP-rajoituksia), kuten esimerkiksi globaalisti levinnyt WannaCry-kiristyshaittaohjelma vuonna 2017 osoitti. Siinä missä valtioilla on monopoli maantieteellisen alueensa sotilaalliseen voimankäyttöön, puuttuu se heiltä kyberturvallisuuden osalta. Tietotekniikan, -järjestelmien ja -verkkojen kattaessa päivä päivältä yhä syvemmin jokaisen elämämme osa-alueen, voivat myös kyberuhat kummuta myös miltä elämän osa-alueelta tahansa. Näin ollen Christensenin & Liebetraun mukaan kyberturvallisuuden omaleimaisina piirteinä voidaan pitää epävarmuutta ja toimijakentän laajaa kattavuutta yksittäisistä henkilöistä valtiollisiin organisaatioihin ja kaikkeen siltä väliltä. (Christensen & Liebetrau 2019, 395-397).

Bay (2016) puolestaan on todennut, että aina kun "kyber”-etuliite lisätään johonkin sanaan, ovat yksityisen sektorin toimijat suurelta osin tämän osa-alueen turvaajia. Täten myöskään analogiat kyberavaruuden ja niin sanotun oikean avaruuden tai tilan välillä eivät ole vedenpitäviä, sillä siinä missä julkinen sektori on usein vastuussa fyysisestä infrastruktuurista, kuten teistä ja voimalaitoksista, ovat puolestaan tietoverkot ja niiden tarvitsema infra lähtökohtaisesti yksityisten toimijoiden vastuulla ja omistuksessa. (Bay 2016, 3).

Pro gradu -tutkielmassani pyrin vastaamaan osaltani kyberturvallisuuden toimijakentän monimuotoisuuden huomioimiseen kriittisen turvallisuudentutkimuksen kontekstissa suuntaamalla analyysini tietoturvakonsulttitalojen diskursseihin valtiollisten toimijoiden sijaan sivuuttamatta teknologista kehitystä tämän diskurssin taustalla. Tietoturvayhtiöiden COVID-19-diskurssi on osaltaan tuottamassa ymmärrystämme siitä, mitä COVID-19-pandemian aikaiselta kyberturvallisuudelta edellytetään, mutta yhtä lailla tämä diskurssi on sidoksissa kontekstiinsa, eli annettuihin etätyömääräyksiin sekä olemassa olevaan teknologiaan, joka mahdollistaa esimerkiksi pilvipalveluiden aiempaa tietoturvallisemman käytön.

Kuvattuani tässä luvussa pro gradu -tutkielmani teoreettista pohjaa, eli sosiaalista konstruktionismia ja sen soveltamista turvallisuudentutkimuksessa, siirryn seuraavassa luvussa tarkemmin avaamaan hyödyntämääni diskurssianalyyttista tutkimusmenetelmää.

3 DISKURSSIANALYYSI JA SEN HABERMASILAINEN SOVELLUTUS – TUTKIMUSMENETELMÄN ESITTELY

Tässä luvussa avaan käyttämäni habermasilaisen diskurssianalyyttisen tutkimusmenetelmän. Luku alkaa diskurssin ja diskurssianalyysin käsitteiden esittelyllä ja jatkuu diskurssianalyysin pääsuuntausten läpikäynnillä. Tämän jälkeen esittelen diskurssianalyysin toteuttamisen Jürgen Habermasin kommunikaation pätevyysvaatimuksia hyödyntämällä, jota pohjustaakseni lyhyesti esittelen Habermasin kommunikatiivisen toiminnan teoriaa. Luvun lopuksi kuvaan, miten tutkielmani pohjalla oleva teoria ja käyttämäni tutkimusmenetelmä nivoutuvat ja tukevat toisiaan.

3.1 Diskurssi ja sen analysointi

Pro gradu -tutkielmani tutkimusmenetelmänä toimii diskurssianalyysi, joka pohjautuu ajatukseen kielenkäytöstä sosiaalista todellisuutta rakentavana sosiaalisena toimintana (Jokinen et al. 2002, 10). Diskurssin käsite on laajasti käytetty monella tieteenalalla ja Fairclough (1997, 31) on erottanut tälle kaksi eri päämerkitystä: kielitieteissä diskurssi ymmärretään ennen kaikkea ihmisten välisenä kanssakäymisenä ja sosiaalisena toimintana, kun taas jälkistrukturalistisiin yhteiskuntateorioihin nojaavassa ajattelussa diskurssi nähdään "todellisuuden sosiaalisena konstruktiona, tiedon muotona". Nämä merkitykset eivät ole toisiaan poissulkevia, vaan kyse on painopiste-eroista, joissa kielitieteellisemmässä lähestymisessä keskiössä ovat yksilöiden välinen vuorovaikutus ja jälkimmäisessä yhteiskunnallisten rakenteiden ja valta-asetelmien vaikutus diskurssien muovautumiselle.

Kummassakin lähestymistavassa kieli, sen käyttö ja käytön ymmärtäminen sosiaalista todellisuutta rakentavana toimintana on keskeinen analyysin kohde. (Suoninen 2002, 18-19). Kielenkäytön analysoinnin keskeisestä merkityksestä huolimatta tutkimussuuntauksesta käytetään kuitenkin termiä diskurssianalyysi

esimerkiksi kielianalyysin sijaan, koska analyysissa ei olla niinkään kiinnostuneita kieliopillisten rakenteiden ja järjestelmien analyysista, vaan millaisiin tarkoituksiin esimerkiksi yksilöt, media, yritykset ja poliittiset puolueet tietämystään kielestä käyttävät ja mitä merkityksiä kielellä tuotetaan (Johnstone 2008, 3).

Diskurssianalyysissa ei ole kyse yhdestä ja samasta tutkimussuuntauksesta, vaan sovellutustapoja ja tutkimuksellisia ratkaisuja on olemassa monia erilaisia (Jokinen & Juhila, 2002, 55). Diskurssianalyysilla on lisäksi läheinen suhde sen sukulaistraditioihin, kuten retoriikan tutkimukseen ja keskusteluanalyysiin. Yhteistä näille suuntauksille on niiden pohjautuminen sosiaaliseen konstruktionismiin teoreettisena viitekehyksenä, tosin kaikilla suhde sosiaaliseen konstruktionismiin ei ole yhtä vahva kuin diskurssianalyysilla. Jokainen näistä suuntauksista jakaa kuitenkin peruslähtökohdan siitä, että tutkimuskohteina ovat kielenkäyttö, teksti ja puhe sellaisenaan ja itsessään, eikä niiden taustalta ole pyrkimystä löytää jotakin "oikeaa" ja objektiivista todellisuutta. Diskurssianalyysille sen sukulaistraditioista erottavana tekijänä on painotus kielen merkityksiä ja sitä kautta sosiaalista todellisuutta rakentaviin käytäntöihin. (Jokinen 2002, 37-38 & 50 ; ks. myös Gralewski 2011).

Remes (2004) on jakanut diskurssianalyyttisen metodologian kolmeen eri koulukuntaan: ranskalaiseen, saksalaiseen ja brittiläiseen. Ranskalaisessa traditiossa tutkimuksen kohteena ovat diskurssien syntymisen ja muovautumisen tavat sekä ympäröivän yhteiskunnan ja kulttuurin legitiimien käytäntöjen rooli ja näkyväksi tekeminen diskurssien synnyssä ja ylläpidossa. Ranskalainen tradition nojautuu vahvasti Michel Foucault'n ajatteluun. Saksalaisessa traditiossa keskiössä on toimijoiden roolin ja aktiivisen keskusteluun osallistumisen merkityksen tutkiminen diskurssin määrittelyssä ja luomisessa väitteiden esittämisen kautta. Saksalaisen tradition keskeinen hahmo on Jürgen Habermas. Pro gradu -tutkielmani tukeutuu nimenomaisesti Habermasin ymmärrykseen vuovaikutuksesta ja hänen kommunikatiivisen toiminnan teoriaansa. Avaan tutkielmani suhdetta tarkemmin Habermasin ajatteluun myöhemmin tässä luvussa. Brittiläisen koulukunnan fokuksena Remeksen mukaan puolestaan on keskustelutapahtuma ja puheen merkitys diskurssin tuottamisessa.

Suonisen (2002, 18) mukaan diskurssianalyysi keskittyy siihen, "millaiset kuvaukset ja selitykset ovat erilaisissa tilanteissa ja keskustelun kohdissa ymmärrettäviä, ja millaisia asiantiloja tai muita seurauksia noilla selityksillä kulloinkin rakennetaan". Toisin sanoen diskurssianalyysissa ei niinkään pyritä löytämään syitä ilmiöille tai ihmisten toiminnalle, vaan siinä analysoidaan tapoja, joilla ihmiset itse kuvaavat toimintaansa, ympäröiviä ilmiöitä, sekä syitä toiminnalleen (Suoninen 2002, 18-19). Diskurssianalyysin keskeisin kysymys on siten *miten* miksi-sanan sijaan, ja tärkeimpänä tehtävän on kuvailu yhteistä sosiaalista todellisuutta rakentavien kulttuuristen merkitysten ymmärtämiseksi positivistiselle lähestymistavalla tyypillisen syiden selvittämisen sijaan (Johnstone 2008, 27; Jokinen & Juhila 2002, 54 ; Juhila & Suoninen 2002, 247). Kuvailevan luonteensa vuoksi diskurssianalyyttinen tutkimus on usein perustutkimuksellista ja sillä on täten itseisarvo tiedon tuottamisessa (Juhila & Suoninen 2002, 244). Tiedon tuottamiseen liittyvän itseisarvonsa lisäksi diskurssianalyysilla on myös muita

käyttötarkoituksia, kuten esimerkiksi yhteiskunnallisen epätasa-arvon tai epäoikeudenmukaisuuden esiin nostaminen.

Tähän liittyy diskurssianalyyttisen tutkimuksen toinen keskeinen jakolinja eli jako analyyttiseen ja kriittiseen diskurssianalyysiin (Jokinen & Juhila 2002, 85-86), jota avaan seuraavaksi tarkemmin.

3.2 Analyyttinen vs. kriittinen diskurssianalyysi

Analyyttisessa diskurssianalyysissa tutkijan pyrkimyksenä on mahdollisimman suuri avoimuus analysoitavalle aineistolle ja sieltä esiin kumpuaville löydöksille ilman ennakko-oletuksia esimerkiksi aineistosta löytyvistä valta- tai alistussuhteista (Jokinen & Juhila 2002, 86). Se kuinka mahdollista tämän pyrkimyksen täyttäminen käytännössä on, on kysymys erikseen. Erona analyyttiselle diskurssianalyysille, kriittiseksi diskurssianalyysiksi kutsutussa suuntauksessa tutkimuksen lähtökohtana yleensä toimii oletus esimerkiksi olemassa olevista alistussuhteista. Tällöin kriittisen diskurssianalyysin tavoitteena on niiden kielellisten käytäntöjen tutkiminen, joilla näitä suhteita tuotetaan, ylläpidetään ja perustellaan. (Jokinen & Juhila 2002, 86). Chouliaraki & Fairclough (1999, 6-16) näkevät, että kriittisen diskurssianalyysin ominaispiirteenä on kielitieteellisen tutkimuksen yhdistäminen kriittiseen yhteiskuntatieteelliseen tutkimusotteeseen, jossa yhdistyy sekä metodisia että teoreettisia elementtejä. Van Dijk (2001, 96) puolestaan on todennut, että kriittinen diskurssianalyysi on aina puolueellista ja tämä tutkimussuuntaus on myös "ylpeä siitä".

Kriittisessä diskurssianalyysissa "puolueellisuus" sekä kriittisyys ilmenevät tutkimuskohteiden valinnassa sekä tutkijan asennoitumisessa tutkimuskohteeseensa. Kriittisessä diskurssianalyysissa keskitytään usein yhteiskunnallisten ongelmien tutkimiseen siitä näkökulmasta, miten diskurssi on tuottamassa ja ylläpitämässä vallitsevia olosuhteita, mutta myös haastamassa vallitsevia ideologioita. Tutkimuksellisena agendana on monesti alistetun tai vähemmistössä olevan ihmisryhmän äänen kuuluville tuominen epätasa-arvoisuuden tuomiseksi näkyville, jotta tähän epäkohtaan voidaan myös puuttua. (Van Dijk 2001, 96 ; Van Dijk 1995, 17-19). Yhteiskunnallisella epätasa-arvolla on vahva sidos turvallisuuteen ja siten myös kyberturvallisuuteen. Mitä ja ketä ollaan turvaamassa ja mitkä ja ketkä jäävät puolestaan tämän turvan ulkopuolella? Entä mitkä toimijat ja tahot nostetaan uhiksi ja mitä vastatoimia näitä vastaan puolestaan määritellään ja perustellaan? Mikä puolestaan on yksilön oikeuksien ja käytettävien valvontateknologioiden välinen tasapaino?

Yhteiskunnallinen epätasa-arvo on vain yksi esimerkki epätasa-arvosta. Tutkimusaiheeni kontekstissa yhtä lailla epätasa-arvoa on siinä, mitä tietoturvariskejä ja toimenpidesuosituksia nostetaan muiden edelle ja kenen etua näiden asioiden eteenpäin vieminen palvelee ja kenen kustannuksella? Tutkielmassani väitän, että tietoturvayhtiöiden julkaisuissa tapahtuvilla diskursiivisilla valinnoilla on iso merkitys sille, millaiseksi kyberturvallisuuskenttä muotoutuu ja

kenen etua ja ääntä sillä palvellaan. Näiden puolien avaamiseksi tarvitaan diskurssianalyysin kriittisiä menetelmiä tutkimusaineiston läpikäymiseksi.

Sisälleen kirjoitetun agendansa vuoksi kriittinen diskurssianalyysi on tutkimuksellisilta lähtökohdiltaan hyvin erilaista verrattuna moneen muuhun tutkimussuuntaukseen, joissa tutkijan agendaa tai puolueellisuutta ei tuoda yhtä eksplisiittisesti esiin tai sitä koitetaan häivyttää. Lisäksi riippumatta siitä, onko kyse kriittisestä tai analyyttisestä diskurssianalyysista, diskurssianalyyttisessä tutkimuksessa ymmärretään tehtävä tutkimus aina myös itsessään tutkittavaksi kohteeksi. Tähän viitataan puhuttaessa diskurssianalyysin refleksiivisyydestä. Tehtävä tutkimustyö yhtä lailla osallistuu sosiaalisen todellisuuden rakentamiseen ja tehdystä tutkimustyöstä tulee uusia tutkimuskohteita tulevalle diskurssianalyyttiselle tutkimukselle. (Juhila 2002, 230).

Kriittisen diskurssianalyysin kolme keskeistä käsitettä ovat Wodakin (2001, 9-11) mukaan kriittisyys, ideologia ja valta. Kriittisyyden käsitteen juuret ovat Frankfurtin koulukunnassa ja kriittisessä teoriassa, mutta käytännössä sillä tarkoitetaan tutkijan etäisyyttä tutkimusaineistoon, ymmärrystä tutkimusaineiston suhteesta ympäröivään yhteiskuntaan sekä tutkijan poliittisen näkökannan tuomista esiin. Ideologialla kriittisen diskurssianalyysin kehikossa tarkoitetaan kielen roolia epätasaisten valtasuhteiden tuottamisessa yhteiskunnassa. Kriittisen diskurssianalyysin näkökulmasta kielellä itsellään ei ole valtaa, vaan tämän vallan se saa siitä, miten valtaapitävät tahot kieltä käyttävät. Tästä syystä kriittisessä diskurssianalyysissa tutkimuskohteena usein on valtaapitävien toimijoiden kielenkäyttö ja vaihtoehtojen esittäminen tälle diskurssille. Ideologian käsite on siten kiinteästi sidoksissa vallan käsitteeseen. Vallan käsite on kriittisen diskurssianalyysin keskiössä, koska kielenkäytöllä voidaan vallan ylläpitämiseksi ja ilmaisemiseksi myös haastaa sitä ja vaikuttaa vallan jakautumiseen.

Pro gradu -tutkielmani lukeutuu kuuluvaksi kriittisen diskurssianalyysin tutkimushaaraan. Tämä siksi, koska en ole tutkielmassani kiinnostunut pelkästään tietoturvayhtiöiden COVID-19 diskurssin kuvailusta, vaan tulen myös pohtimaan ja problematisoimaan sitä, mitä mahdollisia seurauksia tällä diskurssilla on niin kyberturvallisuuspalveluita tarvitseville organisaatioille, heidän henkilöstölle sekä näitä palveluita tarjoaville tietoturvakonsulteille itselleen ja millaiseksi diskurssi muovaa näiden toimijoiden välisiä valtasuhteita.

3.3 Habermasin kommunikatiivisen toiminnan teoria ja siihen pohjautuva diskurssianalyysi

Tutkielmassani tietoturvakonsultointiyhtiöiden COVID-19-diskurssin analyysi- ja luokittelutapana toimii Jürgen Habermasin kommunikatiivisen toiminnan teoriaan tukeutuva kriittisen diskurssianalyysin sovellutustapa, joka perustuu Habermasin teoriassaan esittämiin kommunikaation pätevyysvaatimuksiin (validity claims). Analyysimenetelmän ymmärtämiseksi on ensin paikallaan käydä

Habermasin kommunikatiivisen toiminnan teorian keskeiset piirteet lyhyesti läpi.

3.3.1 Kommunikatiivisen toiminnan teoria

Jürgen Habermasin ajattelun perusteet ovat kriittisestä teoriastaan tunnetusta 1930-luvulla toimintansa aloittaneessa niin sanotussa Frankfurtin koulukunnassa. Koulukunnan keskeinen näkemys oli, että toisin kuin positivismissa, sosiaalisista ilmiöistä ei ole mahdollista tehdä neutraaleja ja puolueettomia kuvauksia. Sen sijaan yhteiskuntateoriat ovat aina joko kriittisiä, eli niiden pyrkimyksenä on epälegitiimien valtasuhteiden esiin tuominen, tai vaihtoehtoisesti nämä teoriat ovat häivyttämässä näiden valtasuhteiden ja niistä seuraavien alistavien olosuhteiden olemassaoloa. (Eiriksen & Weigård 2003, 5). Frankfurtin koulukunnan edustajat valitsivat ensimmäisen lähestymistavan ja siitä nimitys "kriittinen teoria".

Habermasin laajan tuotannon pääteoksena pidetään kaksiosaista *The Theory of Communicative Action (*1984 & 1989). Nimensä mukaisesti teoksen keskeisimmät käsitteet ovat *kommunikatiivinen toiminta* sekä *kommunikatiivinen rationaalisuus.* Kommunikatiivisella rationaalisuudella Habermas tarkoittaa yksilöiden välisessä vuorovaikutuksessa läsnä olevaa rationaalisuutta, joka on välttämätöntä yhteiskunnan instituutioiden, normien ja toimintatapojen ylläpitämiseksi. Rationaalisuuden käsite on täten Habermasille vahvasti sidoksissa myös yhteiskunnassa läsnä oleviin eettisiin ja moraalisiin kysymyksiin. Tämä ymmärrys rationaalisuudesta muodostaa pohjan Habermasin kommunikatiivisen toiminnan ja sen teorian käsitteille. Habermas näkee ihmisten välisen kommunikaation olevan puheakteja (joiden käsitettä kävimme tarkemmin läpi jo edellä kriittisen turvallisuudentutkimuksen ja turvallistamisteorian yhteydessä), eli puhe on teko, jolla saatetaan asioita tapahtumaan. Kommunikatiivisen toiminnan teorian mukaisesti ihmisten välinen kommunikaatio koostuu myönteisten tai kielteisten kantojen ottamisesta kommunikaatiossa läsnä oleviin pätevyysvaatimuksiin. Toisin sanoen kommunikaatiossa mukana olevien osapuolten kommunikaatiosta seuraava toiminta riippuu siitä, miten osapuolet suhtautuvat ja arvioivat toistensa esittämiä lausumia. Kommunikatiivinen toiminta on Habermasille nimenomaisesti yhteistyöhön perustuvaa toimintaa, jonka perusteena on kommunikaatiossa mukana olevien osapuolten yhteisymmärrys kommunikaation pätevyysvaatimuksista. (Eiriksen & Weigård 2003, 4).

Habermas on nimennyt kommunikaatiolle neljä pätevyysvaatimusta, jotka ovat *totuus*, *oikeellisuus, vilpittömyys*[1] ja *ymmärrettävyys*. Totuuden pätevyysvaatimuksella tarkoitetaan sitä, että kommunikaatioon osallistuvan lausuma on sisältönsä osalta tosi. Oikeellisuudella viitataan siihen, että lausuma on suhteessa

[1] Vilpittömyyden pätevyysvaatimuksesta käytetään kirjallisuudessa myös käännöstä *totuudellisuus*, mutta väärinymmärrysten välttämiseksi totuuden ja totuudellisuuden pätevyysvaatimusten välillä, käytän pro gradu -tutkielmassani jälkimmäisestä käännöstä *vilpittömyys*.

normatiiviseen kontekstiinsa oikeutettu. Vilpittömyydellä puolestaan tarkoitetaan sitä, että lausuma on totuudenmukainen ja vilpitön suhteessa lausuman esittäjän tarkoitusperiin. Ymmärrettävyyden vaatimus kattaa lausuman kieliopillisen ja kontekstuaalisen oikeudellisuuden ja ymmärrettävyyden. (Edgar 2005, 148-149 ; Kangas 1989, 40-43).

Siinä missä pätevyysvaatimusten mukainen toiminta on Habermasille kommunikatiivista toimintaa, on puolestaan sellainen toiminta, jossa pätevyysvaatimuksissa on häiriöitä, Habermasin terminologiassa *strategista toimintaa*. Näin ollen kommunikatiivisen toiminnan keskiössä on yhteisymmärrykseen pohjautuva yhteistyö, mutta strategisessa kommunikaatiossa vallalla ovat puhujan itsekeskeiset laskelmat ja vaikutusyritykset oman päämäärän edesauttamiseksi. (Kangas 1989, 46). Kommunikatiivisen ja strategisen toiminnan välimallina on *heikko* kommunikatiivinen toiminta. Vahvassa kommunikatiivisessa toiminnassa totuuden, oikeellisuuden sekä vilpittömyyden pätevyysvaatimukset täyttyvät kommunikaation osapuolten välillä, mutta heikossa ainoastaan totuuden ja vilpittömyyden. Heikko kommunikatiivinen toiminta mahdollistaa kuitenkin osapuolten välisen ymmärryksen, vaikka se ei tuotakaan pitävää sopimusta osapuolten välille samoin kuin vahva kommunikatiivinen toiminta. (Eiriksen & Weigård 2003, 40-44).

Diskurssianalyyttisestä näkökulmasta Habermasille diskurssissa on kyse kahden toimijan välisestä kommunikaatiosta, jonka ylimpänä muotona on ideaali puhetilanne, missä kommunikaatioon osallistuvat toimijat voivat vapaasti jakaa ajatuksiaan ja arvioida toistensa väitteitä ilman pakottavien ja hegemonisten valtatekijöiden läsnäoloa. Ideaalista luonteestaan johtuen tällaiseen kommunikaatioon sen puhtaimmassa muodossa ei osapuolten välisestä vallan epätasapainosta johtuen käytännössä koskaan ole mahdollista päästä. Sen sijaan kommunikaatiossa on aina mukana häiriöitä, eli se on ainakin osittain Habermasin termein strategista kommunikaatiota. Kommunikaatiossa olevat häiriöt eivät kuitenkaan automaattisesti kerro siitä, että kommunikaatioon osallistujat tahallisesti tai pahantahtoisesti haluaisivat rikkoa sitä. (Edgar 2005 , 153-155 ; Koerber 2008, 375-376.)

Kommunikaation häiriöt voivat olla sitä vastoin joko tiedostamattomia tai tiedostettuja kommunikaatioon osallistuvien hegemonisia keinoja ja pyrkimyksiä. Tiedostetulla hegemonisella osallistumisella kommunikaatiossa, jota voidaan kutsua myös tiedostetuksi harhautukseksi, tarkoitetaan kommunikaation aktiivista ja tahallista manipulointia, jolla tähdätään puhujan todellisten pyrkimysten ja tavoitteiden peittämiseen. Tiedostamattomalla osallistumisella tai harhautuksella tarkoitetaan puolestaan hallitsevien ideologioiden sisällyttämistä kommunikaatioon puhujan näitä kyseenalaistamatta, eli tilannetta, jossa puhuja itsekään ei tiedosta vievänsä kommunikaatiota kauemmas ideaalista puhetilanteesta. (Wall et al. 2015, 261.) Eronteko tiedostetulle tai tiedostamattomalla harhautukselle on haastavaa ellei mahdotonta ilman syvempää perehtymistä kommunikaatioon osallistujan tarkoitusperiin pelkän kirjoitetun tai suullisen puheen analysoimisen sijaan. Pro gradu -tutkielmassani en ole kiinnostunut siitä, onko kyseessä tiedostettu vai tiedostamaton kommunikaation harhautus, vaan pyrin

tunnistamaan näitä mahdollisia häiriöitä niiden tahallisuudesta riippumatta. Keinoina näiden häiriöiden tunnistamiseen on Habermasin pätevyysvaatimuksiin tukeutuva diskurssianalyysi, jonka toteutusperiaatteita avaan seuraavaksi.

3.3.2 Kommunikaation pätevyysvaatimukset diskurssianalyysin lähtökohtana

Habermasin kommunikatiivisen toiminnan teorian alkuperäisenä painopisteenä oli institutionaalisten toimijoiden, kuten median ja suuryritysten, roolin ja merkityksen tarkastelu julkisen keskustelun ja diskurssien muovaamisessa demokraattisessa yhteiskunnassa. (Cukier et al. 2009, 176-177). Pro gradu -tutkielmani kytkeytyy näihin perinteisiin, sillä analyysini kohteena on suurten monikansallisten tietoturvayhtiöiden käyttämä kieli. Tämän kielen ja siinä vallalla olevien diskurssien analysoimiseksi hyödynnän neljää edellä mainittua Habermasin kommunikaation pätevyysvaatimusta.

Habermasin määrittelemää neljää kommunikaation pätevyysvaatimusta voidaan hyödyntää diskurssianalyysin tekemiseen esimerkiksi sen arvioimiseksi miten teknologisia, tieteellisiä tai asiantuntijuutta koskevia totuuksia tuotetaan (Koerber et al. 2008, 364). Pro gradu -tutkielmassani kiinnostuksen kohteena on tietoturvaa koskevien totuuksien ja ymmärryksen tuottaminen COVID-19-pandemian kontekstissa.

Tarkemmin ottaen tutkimusmenetelmänäni käyttämä habermasilainen diskurssianalyysi pohjautuu Cukier et al. (2009) esittämään diskurssianalyysin sovellustapaan, jossa tutkimusaineistoa analysoidaan vasten näitä neljää kommunikaation pätevyysvaatimusta. Cukier et al. omassa tutkimuksessaan analysoivat Acadia Advantage -nimisen kanadalaisten yliopistojen teknologihankkeen uutisointia tiedotusvälineissä. Tietojärjestelmätieteiden saralla Habermasin kommunikatiivisen toiminnan teoriaan pohjautuvaa tutkimusta on tehty myös tätä ennen (ks. esim. Lyytinen 1992 ; Lyytinen & Hirschheim 1988) ja myös tietoturvallisuuden tutkimuksen puolella Habermasin pätevyysvaatimuksia on hyödynnetty esimerkiksi tietoturvapolitiikkojen diskurssien analysoimisessa (ks. Stahl et al. 2012).

Cukier et al. (2009) omassa tutkimuksessaan olivat kiinnostuneita Acadia Advantage -hankkeen uutisoinnista löytyneistä kommunikatiivisista häiriöistä, jotka ohjasivat ymmärrystä hankkeesta sen läpivientiä suosivaan suuntaan korostamalla esimerkiksi hankkeesta saatavia hyötyjä siitä aiheutuvien kustannusten sijaan. Stahl et al. (2012) Iso-Britannian terveydenhuollon tietoturvapolitiikkojen osalta olivat puolestaan kiinnostuneita niistä löytyvistä ideologiosta ja hegemonioista, joiden löytämiseksi he analysoivat aineistoa Habermasin neljää pätevyysvaatimusta vasten. Stahlin et al. ymmärryksessä ideologiat ovat tiettyjä jaettuja ja kyseenalaistamattomia ymmärryksiä sosiaalisesta todellisuudesta. Hegemonia heille puolestaan on menetelmä tai mekanismi, jolla tiettyä ideologiaa pidetään yllä. Esimerkiksi teknisen jargonin käyttö tietoturvapolitiikoissa on

heidän mukaansa esimerkki hegemoniasta, joka pyrkii pitämään yllä ideologiaa tietoturvasta teknisten asiantuntijoiden valta-alueena. (Stahl et al. 2012, 79 & 86). Oman tutkielmani osalta olen kiinnostunut tunnistamaan sekä kommunikaatiosta löytyviä mahdollisia häiriöitä että löytämään esimerkkejä ideologioiden ja hegemonioiden läsnäolosta, jotka auttavat paremmin ymmärtämään kyberturvallisuuteen liittyviä valtarakenteita.

Esimerkkejä kommunikatiivisista häiriöistä ovat esimerkiksi ilman perusteita esitetyt totuudenomaiset väitteet tai runsas adjektiivien käyttö, jotka painottavat asian tiettyä puolta muiden kustannuksella. Perusteettoman totuusväitteen esittäminen saattaa olla samalla esimerkki myös hegemoniasta, jolla tätä väitettä pyritään tuottamaan kyseenalaistamattomaksi ja yhteisesti jaetuksi tosiasiaksi, jonka kaikki hyväksyvät myös ilman perusteita. Kommunikatiivisten häiriöiden, ideologioiden ja hegemonioiden tunnistamiseksi jokaisen pätevyysvaatimuksen kohdalla aineistolle on esitettävä omat sitä koskevat kysymyksensä.

Totuuden pätevyysvaatimuksessa keskitytään siihen, onko kommunikaation sisältö totta ja perustuuko se faktoihin vai onko se vääristeltyä ja puolueellista. Vaatimuksenmukaisuuden tarkistamiseksi tulee selvittää, millaisia vaihtoehtoja kuulijalle esitellään, miten ne on määritelty ja millaisia todisteita ja perusteita näiden tueksi esitellään. (Cukier et al. 2004, 239-242 ; Cukier et al. 2009, 178-180).

Vilpittömyyden osalta kommunikaation analysoijaa kiinnostaa puhujan rehellisyys ja johdonmukaisuus. Vaatimuksenmukaisuuden arvioimiseksi analyysin keskiössä ovat esimerkiksi käytetyt vertauskuvat ja adjektiivit, joilla kuulijaa voidaan johtaa harhaan tai joilla tiettyjä puolia viestistä voidaan yrittää hämärtää. Lisäksi tarkastelun kohteeksi tulee ottaa se, mitä puhuja sanoo, miten hän sen sanoo ja mitä puhuja lopulta tekee, sekä näiden kolmen yhdenmukaisuus. (Cukier et al. 2004, 241 ; Cukier et al. 2009, 180-181).

Oikeellisuuden pätevyysvaatimuksella Habermas tarkoittaa puhujan sanojen suhdetta vallitseviin normeihin ja arvoihin. Vaatimuksen toteutumisen arvioimiseksi täytyy keskittyä siihen, kenen ääni ylipäätään on kuuluvilla ja kenen puolestaan tukahdutetaan ja jätetään kuulumattomiin. Tärkeänä kommunikaation oikeellisuuden arvioinnin kriteerinä on myös se, mihin tahoihin puheessa viitataan asiantuntijoina ja millä perusteilla. Näitä tekijöitä analysoimalla voidaan saada selville, kenen äänet ja mahdolliset näkemykset diskurssissa puuttuvat. (Cukier et al. 2004, 241 ; Cukier et al. 2009, 181).

Ymmärrettävyyden vaatimuksen kohdalla puolestaan keskitytään siihen, ymmärtävätkö puhuja ja kuulija toisiaan. Onko käytetty kieli esimerkiksi johdonmukaista ja kontekstualisoidaanko välitettyä viestiä miten? Entä sisältääkö teksti teknistä jargonia tai muuten vaikeasti ymmärrettävää terminologiaa? Ymmärrettävyyden vaatimusta voidaan rikkoa puutteellisen kommunikaation lisäksi liiallisella määrällä informaatiota, jonka oikeaksi ymmärtämiseksi kuulijalla ei ole mahdollisuuksia. (Cukier et al. 2004, 241 ; Cukier et al. 2009, 179 ; Graber 2017, 297).

Pro gradu -tutkielmani osalta tutkimusaineistolle pätevyysvaatimuksittain esitetyt kysymykset on kuvattu taulukossa 1. Näiden kysymysten kautta

puolestaan saadaan vastaukset myös tutkielman johdannossa esitettyihin tutkielman päätutkimuskysymyksiin.

Pätevyysvaatimus	Tietoturvayhtiöiden julkaisuille esitetyt kysymykset
Totuus	• Mitä COVID-19-pandemian vaikutuksista sanotaan tietoturvalle? • Esitetäänkö COVID-19-pandemian vaikutuksille vaihtoehtoja ja jos, niin minkälaisia? • Millaisiin todisteisiin esitetyt väittämät perustuvat?
Oikeellisuus	• Mitä tietoturvariskejä ja -uhkia COVID-19-pandemiaan liittyen korostetaan? • Mitä toimenpidesuosituksia COVID-19-pandemiaan liittyen korostetaan? • Kenen ääni puheessa on kuuluvilla? • Ketkä ja mitkä asiat kommunikaatiosta jäävät puuttumaan?
Vilpittömyys	• Millaisia adjektiiveja ja muita kuvailevia ilmauksia julkaisuissa käytetään? • Ohjaavatko nämä ymmärrystä COVID-19-pandemian vaikutuksista tietoturvalle johonkin tiettyyn suuntaan?
Ymmärrettävyys	• Käytetäänkö julkaisuissa teknistä jargonia tai muuta epäselvää terminologiaa?

TAULUKKO 1. Kysymykset aineistolle pätevyysvaatimuksittain (mukaillen Stahl et al. 2012).

3.4 Yhteenveto teoreettisesta kehyksestä ja tutkimusmenetelmästä

Luvuissa 2 ja 3 olen käynyt läpi tutkielmani teoreettisen viitekehyksen sekä käyttämäni tutkimusmenetelmän. Yhteenvetona tutkielmani teoreettisena taustana toimii sosiaalinen konstruktionismi, eli ymmärrys todellisuudesta ihmisten välisessä vuorovaikutuksessa rakentuvana. Jotta tämän ymmärryksen valossa todellisuutta voidaan tutkia, täytyy analyysi kohdistaa ihmisten väliseen vuorovaikutukseen eli kielenkäyttöön. Tutkimusmenetelmää, jossa tutkitaan kielenkäytössä rakentuvia merkityksiä, kutsutaan diskurssianalyysiksi. Oma tutkielmani lukeutuu tutkimusmenetelmän käytön osalta diskurssianalyysin kriittiseen suuntaukseen. "Kriittinen " etuliitteenä on edellä ollut diskurssianalyysin lisäksi tutkielmassani esillä puhuttaessa kriittisestä teoriasta sekä kriittisestä

turvallisuudentutkimuksesta. Kriittisyydellä näissä kaikissa yhteyksissä tiivistetysti tarkoitetaan sitä, että ihmisten väliseen vuorovaikutukseen liittyy aina vallankäyttöä sekä vallan epätasaista jakautumista. Tämän vallankäytön näkyväksi tuominen on kriittisen tutkimuksen tarkoitus.

Diskurssianalyysissa tai sen kriittisessä haarassa ei ole kyse yhdestä ja samasta tutkimusmenetelmästä, vaan diskursseja voidaan analysoida hyvin monella eri tavoin. Pro gradu -tutkielmassani analyysitavaksi on valikoitunut Habermasin kommunikatiivisen toiminnan teoriaan pohjautuva diskurssianalyysi, jossa diskurssia tarkastellaan Habermasin neljän kommunikaation pätevyysvaatimuksen – totuuden, vilpittömyyden, oikeellisuuden ja ymmärrettävyyden – kautta. Tiivistelmä tutkielman taustalla olevasta teoriasta ja käytetystä tutkimusmenetelmästä on esitettynä myös kuviossa 1.

KUVIO 1 Tutkielman teoreettinen ja metodologinen kehys.

Toisin sanoen tutkimuskysymysteni kontekstissa tutkielmassani ollaan kiinnostuneita siitä, millaista ymmärrystä kyberturvallisuudesta, sen tarpeesta, sitä koskevista uhkista ja tarvittavista suojautumiskeinoista tietoturvayhtiöiden COVID-19-diskurssilla ollaan tuottamassa. Tutkimusotteen kriittisyys tulee esille siinä, että tutkielmassa pyritään analysoimaan sitä, kenen ääni diskurssissa on kuuluvilla ja mitä agendaa sillä mahdollisesti pyritään ajamaan eteenpäin sekä vastavuoroisesti sitä, kenen ääni diskurssissa jää mahdollisesti kuulumattomiin. Habermasilaisen diskurssianalyysin mukaisesti tietoturvayhtiöiden COVID-19-diskurssia arvioidaan tutkielmassa neljän kommunikaation pätevyysvaatimuksen kautta. Tämä tarkoittaa sitä, että tutkimusaineistosta analysoidaan siinä esitettyjä totuusväittämiä (totuuden pätevyysvaatimus), sitä kenen ääni

aineistossa on kuuluvilla ja millaisiin asiantuntijoihin julkaisuissa esimerkiksi viitataan (oikeellisuuden pätevyysvaatimus) sekä käytettyjä vertauskuvia ja adjektiiveja (vilpittömyyden pätevyysvaatimus) Neljänneksi aineistosta analysoidaan käytettyä jargonia sekä muuta terminologiaa, joka voi estää tai rajata julkaisujen ymmärtämistä (ymmärrettävyyden pätevyysvaatimus).

Seuraavassa luvussa käydään tarkemmin läpi tutkielmassa käytettävä tutkimusaineisto sekä sen analysoimisessa huomioon otettavat erityispiirteet.

4 TUTKIMUSAINEISTON ESITTELY

Tässä luvussa esitellään tutkielmassa tutkimusaineistona käytettävät tietoturvakonsultointiyhtiöiden julkaisut, miten ne on kerätty ja rajattu sekä miten aineistoa tullaan analysoimaan.

4.1 Tutkimusaineiston tuottaneet tietoturvakonsultointiyhtiöt

Pro gradu -tutkielmani tutkimusaineistona toimii kahden tietoturvakonsultointiyrityksen –Deloitten ja PwC :n – vuoden 2020 aikana heidän kotisivuillaan julkaistut[2] raportit, artikkelit, blogikirjoitukset sekä muut julkaisut, jotka käsittelivät tietoturvaa ja tietoturvasuosituksia COVID-19-pandemian aikana. Podcastit ja videomuodossa olevan materiaalin rajasin aineiston ulkopuolelle, ellei näiden sisällöstä ollut saatavilla myös kirjallista transkriptiota. Aikarajauksena aineistolle käytin maalis–joulukuuta 2020. Aikarajauksen perusteena on globaalien COVID-19-pandemiaa koskevien rajoitustoimien alku maaliskuussa 2020 sekä tutkimusaineiston kerääminen tammikuun 2021 aikana, jonka takia tätä uudemmat julkaisut eivät ehtineet analyysiin mukaan. Aikajakso riittää kuitenkin kattamaan pandemiasta aiheutuneiden rajoitustoimien alun, niiden osittaisen purkamisen kesällä 2020 sekä uudelleen määräämisen syksyllä 2020. PwC:n osalta kaikissa julkaisuissa ei ollut tarkkaa päivämäärämerkintä. Tämän takia PwC:n osalta aineisto on vuoden 2020 osalta käyty läpi kokonaisuudessaan COVID-19-aiheisten tietoturvajulkaisujen löytämiseksi.

Deloitten ja PwC:n aineistoksi valikoitumisen taustalla oli tutkimuslaitos Forresterin globaaleja tietoturvakonsultointiyhtiöitä koskeva vertailu vuodelta 2019, jossa Deloitte ja PwC olivat kaksi johtavimmassa asemassa olevaa toimijaa (Forrester 2019). Molemmat valituista yrityksistä ovat monikansallisia toimijoita. Deloitten palveluksessa oli vuoden 2020 tilastojen mukaan noin satatuhatta

[2] Osa raporteista edellytti rekisteröitymistä eli yhteystietojen antamista, jotta ne oli mahdollista ladata ja lukea.

työntekijää ja PwC:llä puolestaan lähemmäs kolmesataatuhatta. Liikevaihdot molemmilla yrityksillä pyörivät muutamissa kymmenissä miljardeissa dollareissa. Tässä yhteydessä on tärkeää huomioida, että näissä numeroissa on mukana kyseisten yritysten kaikki liiketoiminta, eikä ainoastaan tietoturvakonsultointi, mikä on vain yksi osa näiden yritysten toimintaa. Sekä Deloitte että PwC kuuluvut niin sanottuihin Big 4 -yrityksiin. Tällä termillä viitataan globaalisti neljään suurimpaan tilintarkastusyhtiöön. Tilintarkastustoiminnan merkittävä rooli näissä yrityksissä on myös alkujaan vaikuttanut näiden tietoturvakonsultointitoiminnan käynnistymiseen, koska yrityksillä on ollut hallussaan suuri määrä luottamuksellista asiakasorganisaatioiden taloustietoa, joka on ollut tarpeen pystyä myös suojaamaan (Sweet 2019).

Sekä Deloitten että PwC:n harjoittaman tietoturvakonsultointiliiketoiminnan osalta on tärkeää painottaa, että molemmat ovat profiloituneet nimenomaan konsultoijina ja neuvonantajina, eivätkä niinkään omien tietoturvateknologioiden kehittäjinä. Näiden yritysten tietoturvakonsultointi perustuu teknologiakumppanuuksiin näitä teknologioita kehittävien toimijoiden kanssa, joiden teknologioiden ympärille he palveluitaan rakentavat ja joiden lisenssejä he rajoitusten puitteissa jälleenmyyvät. Rajoituksilla viittaan siihen, että näiden yritysten harjoittama tilintarkastustoiminta asettaa tiettyjä ehtoja sille, kenen toimijoiden kanssa he voivat yhteistyötä tehdä. Tiivistetysti tilintarkastustoiminnasta periytyy riippumattomuuden periaate myös näiden yritysten konsultointitoimintaan, jonka vuoksi nämä yritykset eivät voi esimerkiksi jälleenmyydä sellaisten teknologioiden lisenssejä, joiden kehittäjille ja valmistajille he itse toimivat tilintarkastajina.

4.2 Aineiston kerääminen

Vaikka Deloitten ja PwC:n kohdalla on kyse monikansallisista yrityksistä, jotka tuottavat aineistoa usealla eri kielellä, on pro gradu -tutkielmassani käytetyn aineiston keräämiseen käytetty ainoastaan näiden yritysten englanninkielisiltä sivuilta löytyvää aineistoa. Aineiston keräämiseen käytetyt URL-osoitteet aineiston keräämishetkellä olivat seuraavat:

- **Deloitte**: www2.deloitte.com/us/en/insights/topics/cyber-risk.html &
  https://www2.deloitte.com/global/en/blog/responsible-business-blog.html
- **PwC**: https://www.pwc.com/gx/en/research-insights.html & https://www.pwc.com/gx/en/issues/cybersecurity.html.

Yritysten kotisivuilta analyysin kohteeksi valikoitunut aineisto on etsitty hakusanoja käyttämällä tai valitsemalla aihealueeksi tietoturva, jonka sisältä julkaisuja on etsitty. Deloitten kohdalla käytettiin aihealuerajausta "cyber risk”,

jonka pohjalta saataville tuli tietoturvaa koskevat julkaisut. Lisäksi Deloitten tietoturvaa koskeville blogikirjoituksille oli oma sivustonsa. PwC:n osalta käytettiin puolestaan sekä hakusanaa "cyber " että aihealuerajausta "cybersecurity ".

Tietoturva-aiheisten julkaisujen löytämisen jälkeen julkaisut käytiin yksitellen läpi viittausten COVID-19-pandemiaan löytämiseksi. Tämä suoritettiin tekemällä sanahaku "covid" julkaisun sisällä. Tässä kohtaa on hyvä huomioida, että alun perin aineiston oli tarkoitus kattaa Deloitten ja PwC:n lisäksi myös kaksi muuta tietoturvakonsultointiyhtiötä. Covid-hakusanalla tehdyn haun jälkeen tutkimusaineistoksi nämä kaksi muuta yhtiötä mukaan lukien oli rajautunut yhteensä 86 tietoturva-aiheista julkaisua, joissa viitattiin myös COVID-19-pandemiaan. Huomioiden pro gradu -tutkielman laajuuden sekä käytettävän diskurssianalyyttisen tutkimusmenetelmän, oli 86 analysoitavaa julkaisu liian suuri määrä. Tämän takia rajausta tarkennettiin julkaisuiden otsikoiden perusteella. Mukaan päätyivät ne artikkelit, joiden otsikossa joko suoraan mainittiin COVID-19 tai niissä muuten viitattiin pandemiaan esimerkiksi mainitsemalla etätyöt tai ”uusi normaali”. Lisärajauksen tekeminen otsikointiin pohjautuen perustui siihen oletamukseen, että jos julkaisujen potentiaalinen lukija haluaa saada tietoa esimerkiksi tietoturvasuosituksista COVID-19-pandemiaan liittyen, avaa hän todennäköisemmin julkaisun, jonka otsikossa on tähän aiheeseen jo suora viittaus.

Otsikkorajauksen jälkeen yksittäisiä julkaisuja oli jäljellä yhteensä 43 kappaletta neljältä yritykseltä. Tehdessäni analyysia kuitenkin havaitsin, että tämä on edelleen liian suuri määrä aineistoa. Tästä johtuen tiputin kaksi muuta alun perin mukana ollutta yritystä pois ja jäljelle jäivät Deloitte ja PwC, jotka Forresterin edellä mainitussa raportissa oli nostettu korkeimmalle johtavien tietoturvakonsultointiyhtiöiden osalta. Lopullisen rajauksen jälkeen jäljellä oli yhteensä 19 julkaisua: Deloittelta 8 ja PwC:ltä 11. Lopullinen lukumäärä on laskettu niin, että jos esimerkiksi yhtiön kotisivuilta löytyneen artikkelin liitteenä on samaa aihetta tarkemmin käsittelevä PDF-raportti, niin tällöin nämä muodostavat kaksi erillistä julkaisua. Tutkielman analyysiosioissa näihin julkaisuihin viitataan yrityksen etukirjaimella ja juoksevalla numerolla. Edellä kuvatun kaltaisessa tilanteessa, jossa artikkelin liitteenä on ollut PDF-raportti, viitataan PDF-raporttiin liittämällä etukirjaimen ja juoksevan numeroon perään ”b”: esimerkiksi merkintä ”D4” koskee artikkelia ja ”D4b” puolestaan sen liitteenä ollutta raporttia. Tarkka luettelo tutkimusaineistona käytetyistä julkaisuista löytyy taulukosta 1 sekä tutkielman lähdeluettelosta.

Viite	**Julkaisun nimi**	**Tyyppi**	**Julkaisupvm.**
D1	New World, New Risk – How COVID-19 Is Transforming Business for the Next Normal	Artikkeli	17.6.2020
D2	COVID-19 Supercharges Cyber	Artikkeli	3.6.2020
D3	The Acceleration of Digitization as a Result of COVID-19	Artikkeli	30.7.2020
D4	States at risk: The cybersecurity imperative in uncertain times	Artikkeli	15.10.2020

D4b	2020 Deloitte-NASCIO Cybersecurity Stydy. States at risk: the cybersecurity imperative in uncertain times	Raportti	15.10.2020
D5	Rebooting risk management. Making risk relevant in a world remade by COVID-19.	Artikkeli	23.9.2020
D5b	Rebooting risk management. Making risk relevant in a world remade by COVID-19.	Raportti	23.9.2020
D6	Reshaping the cybersecurity landscape. How digitization and the COVID-19 pandemic are accelerating cybersecurity needs at many large financial institutions.	Artikkeli	24.7.2020
P1	Cyber security strategy 2021 – An urgent business priority	Artikkeli	-
P1b	Global Digital Trust Insights Survey 2021	Raportti	-
P2	How fake news has exploited COVID-19	Artikkeli	-
P3	How to maintain your cyber security awareness programme with a remote workforce	Blogi	1.7.2020
P4	Why has there been an increase in cyber security incidents during COVID-19?	Artikkeli	-
P5	SWIFT CSP controls and remote working practices – This might be the time to revisit SWIFT CSP controls in the context of remote working practices due to COVID-19	Artikkeli	-
P6	Digital Identity supports a secure remote digital workforce during COVID-19	Artikkeli	-
P6b	Digital Identity supports a secure remote digital workforce during COVID-19	Raportti	-
P7	COVID-19: Making remote work productive and secure	Artikkeli	-
P8	How to protect your companies from rising cyber attacks and fraud amid the COVID-19	Artikkeli	-
P9	How to manage the impact of COVID-19 on cyber security	Artikkeli	24.3.2020
P9b	Managing the impact of COVID-19 on cyber security	Raportti	20.3.2020

Taulukko 2. Analysoidut tietoturvakonsultointiyhtiöiden julkaisut.

4.3 Aineiston kuvailu

Tietoturvakonsultointiyhtiöiden julkaisuja voidaan tutkimusaineistotyypiltään kutsua niin sanotuksi harmaaksi kirjallisuudeksi. Harmaalla kirjallisuudella tarkoitetaan julkaisuja, jotka on julkaissut jokin ei päätoimisesti julkaisutoimintaa harjoittava toimija, ja jotka eivät ole käyneet läpi tieteellisten julkaisujen vertaisarviointiprosesseja. Tällaisia julkaisuja ovat esimerkiksi julkishallinnon, oppilaitosten sekä yritysten tekemät tiedotteet, uutiskirjeet, raportit, hallinnolliset asiakirjat, työpaperit ja muut vastaavat julkaisut. (Adams et al. 2017, 433-434 ;

Rothstein & Hopewell 2009, 104-105). Kiinnostavan alalajinsa teknologia-alan toimijoiden julkaisuista muodostavat white paper -julkaisut. Nämä julkaisut ovat Harveyn & Branco-Illodon (2020, 116) mukaan teknisten raporttien ja manifestien välissä, sillä ne usein esittelevät jonkin uuden teknisen innovaation, mutta samalla ne myös tarjoavat ratkaisuehdotuksia johonkin konkreettiseen ongelmaan, mikä voi tapahtua esimerkiksi kirjoittajan esittelemän uuden teknologian avulla. Tutkimusaineistossa white paper -tyyppisiä julkaisuja on mukana yksi kappale, PwC :n digitaalisen identiteetin merkitystä etätöiden sujuvoittamisessa ja turvaamisessa käsittelevä julkaisu (P6b).

Harmaaksi kirjallisuudeksi luokiteltuja julkaisuja on tieteellisen tutkimuksen teon yhteydessä välillä kritisoitu epäluotettaviksi ja laadultaan tieteellisiä vertaisarvioituja julkaisuja heikommiksi (Rothstein & Hopewell 2009, 120). Tämä saattaisi olla haaste, jos pro gradu -tutkielmassani näitä julkaisuja käytettäisiin tieteelliseen tutkimuskirjallisuuteen rinnasteisesti. Pro gradu -tutkielmassani tietoturvayhtiöiden julkaisut toimivat tämän sijaan itsessään diskurssianalyysin kohteena, joten näiden julkaisujen mahdollisella "epätieteellisyydellä" ei tutkielmani kannalta ole merkitystä.

Kuten jo todettua, tutkimuksen kohteena oleva aineisto on julkisesti saatavilla kummankin tietoturvayhtiön kotisivuilta. Aineiston julkisuus ei kuitenkaan tarkoita, että aineisto ja niiden sisältämä viesti olisi suunnattu kenelle tahansa. Tietoturvayhtiöiden julkaisujen tärkeimpänä yleisönä on heidän nykyinen tai tuleva potentiaalinen asiakaskuntansa, eli sekä yksityisen että julkisen sektorin organisaatiot ja niissä tietoturvasta vastaavat henkilöt. Tämän kaltaisia julkaisuja voidaan käyttää suoraan joko markkinoinnin, myynnin tai konsultoinnin tukena, mutta niillä on keskeinen rooli myös yrityskuvan eli yrityksen brändin kannalta. Tuotteiden tai palveluiden laadulla kilpaileminen ja erottautuminen on koko ajan vaikeampaa, minkä takia yritysten herättämien mielikuvilla on kasvava merkitys (Todor 2014, 59). Tietoturvayhtiöiden julkaisut ovat osaltaan rakentamassa näitä mielikuvia, ennen kaikkea mielikuvaa yhtiöiden asiantuntijuudesta tarjoamiensa palveluiden saralla.

4.4 Kvalitatiivisen aineiston analysointi

Valitsemani tutkimusaineiston ja tutkimusmenetelmän myötä pro gradu -tutkielmani on kvalitatiivista tutkimusta, jonka tunnuspiirteitä ovat analyysissa keskittyminen havainnointiin, kuvailuun ja tulkintaan unohtamatta oman henkilökohtaisen, yhteiskunnallisen ja kulttuurisen kontekstimme vaikutusta tekemillemme tulkinnoille (Bazeley 2021, 6-7). Hirsjärven et al. (2007, 157) mukaan "kvalitatiivisessa tutkimuksessa pyritään tutkimaan kohdetta mahdollisimman *kokonaisvaltaisesti* (kursivointi alkuperäinen)". Tällä he tarkoittavat sitä, että kvalitatiivisessa tutkimuksessa tutkittavaa todellisuutta ei voi paloitella pienemmiksi paloiksi aivan miten huvittaa, vaan nämä palaset muovaavat ja ovat toisiinsa suhteessa siten, että näiden muodostama kokonaisuus tulee myös huomioida.

Bazeley (2021, 7) on lisäksi nimennyt kvalitatiivisen tutkimuksen yhdeksi perusominaisuudeksi sen tapausluonteisuuden ja -tutkimuksellisuuden. Käsitteellisesti tapaukset voidaan jakaa teoreettisiin sekä empiirisiin tapauksiin. Teoreettisella tapauksella tarkoitetaan sitä ilmiötä, mistä johtopäätöksiä ollaan tekemässä ja empiirisillä tapauksilla puolestaan niitä yksiköitä, mistä data kerätään ja analysoidaan. (Bazeley 2021, 7-9). Pro gradu -tutkielmani kohdalla teoreettinen tapaus on kyberturvallisuuden COVID-19-diskurssi ja empiirisinä tapauksina puolestaan toimivat valitsemani kahden eri tietoturvakonsulttiyhtiön julkaisemat raportit, blogit ja artikkelit.

Bazeley (2021, 14-19) on jakanut kvalitatiivisen tutkimusprosessin neljään päävaiheeseen. Näistä ensimmäinen on analyysiin valmistautuminen. Tässä vaiheessa tutkija ottaa selvää mahdollisista tutkimusmenetelmistä, arvioi tapausten keskeisyyttä tutkittavan ilmiön kannalta, ymmärtää tutkimuksen tieteenfilosofiset perustat, perehtyy miten muut tutkijat aiemmin ovat lähestyneet vastaavankaltaisia tutkimuskysymyksiä sekä laatii menetelmät tutkimusaineistonsa hallinalle. Toisessa vaiheessa alkaa aineiston analysointi, joka kattaa aineiston lukemisen ja reflektoinnin, aineistosta nousevien teemojen luokittelun ja yhdistelyn sekä jatkuvan arvioinnin ja uudelleen läpikäynnin jo tehtyjen löydösten laadun varmistamiseksi. Kolmannessa vaiheessa alkaa varsinainen kirjoitustyö sisältäen aineiston kuvailun, vertailun ja yhdistämisen jo aiemmin tehtyyn tutkimukseen. Viimeisessä vaiheessa analyysi viimeistellään selittämällä tehtyjen havaintojen ja löydösten merkityksellisyys, terävöittämällä tehtyjen johtopäätösten yhteyttä tutkimusaineistoon sekä pohtimalla tutkimuksen tulosten merkitystä ja sovellettavuutta oman tutkimusasetelman ulkopuolelle. Tämän nelivaiheisen prosessin tuloksia omien tutkimuskysymyksieni osalta käydään läpi seuraavassa kolmessa analyysiluvussa ja niitä seuraavassa tutkielman päättävässä tulos- ja johtopäätösluvussa.

5 TOTUUDEN PÄTEVYYSVAATIMUS

Tässä luvussa tarkastellaan tutkimusaineistona olleiden tietoturvakonsultointiyhtiöiden COVID-19-aiheisten tietoturvajulkaisujen totuusväittämiä. Totuusväittämillä tarkoitan niitä artikkeleista löytymiä lausumia, joilla esimerkiksi kuvataan millainen COVID-19-pandemian vaikutus on ollut organisaatioiden tietoturvallisuudelle ja mitä organisaatioiden tulisi tässä tilanteessa näiden yhtiöiden mukaan tehdä.

Habermasin kommunikatiivisen toiminnan teoriaan tukeutuvassa diskurssianalyysissa ollaan aiemmassa tutkimuksessa (ks. esim. Cukier et al. 2009, Stahl et al. 2012 & Graber 2017) oltu vahvasti kiinnostuneita myös siitä, millaisiin perusteisiin ja todisteisiin totuuslausumat ovat pohjautuneet. Analyysissa tullaan arvioimaan myös tätä puolta, mutta tarkemmassa keskiössä on se, millaista sosiaalista todellisuutta aineistosta löytyvillä totuuslausumilla COVID-19-pandemian vaikutuksista kyberturvallisuudelle rakennetaan. Käyttämällä kieltä tietyllä tavalla ja muodostamalla "totuuksia" on mahdollista painottaa asioiden tiettyjä puolia ja samalla peittää joitakin toisia puolia samasta asiasta (Lämsä 2014). Lisäksi analyysissa tullaan pohtimaan mitä mahdollisia seurauksia valituilla totuuslausumilla ja kielenkäytöllä on sekä julkaisut laatineille tietoturvayhtiöille itselleen että julkaisujen lukijoille.

5.1 COVID-19 ennalta-arvaamattomana ja radikaalina uhkia kasvattaneena muutoksena

Ensimmäisenä tarkastelluista tietoturvayhtiöiden julkaisuista esiin nouseva totuusväittämä liittyy COVID-19-pandemian suureen ja jopa radikaaliin merkitykseen organisaatioiden kyberturvallisuudelle. COVID-19-pandemian suuri merkitys kyberturvallisuudelle käy ilmi jo artikkelien ja raporttien otsikoinneista, joista löytyy esimerkiksi seuraavia nimiä: *COVID-19 Supercharges Cyber* (D2), *Reshaping the cybersecurity landscape: How digitization and the COVID 19 pandemic are*

accelerating cybersecurity needs at many large financial institutions (D6) ja *How to protect your companies from rising cyber attacks and fraud amid the COVID-19 outbreak* (P8). Otsikot rakentavat täten ymmärrystä COVID-19-pandemiasta sekä kyberturvallisuuden merkitystä että kyberriskejä kasvattaneena tapahtumana. Suuren merkityksenä lisäksi COVID-19:n mukana tuoma toimintaympäristö, erityisesti kasvaneiden etätöiden osalta, näyttäytyy tutkimusaineistossa myös ennalta-arvaamattomana, äkillisenä sekä täynnä epävarmuutta olevalta, mitä seuraavat esimerkkisitaatit havainnollistavat:

> Some companies plan for regional work-from-home scenarios caused by natural disasters, geopolitical events and other disruptions, but the concept of *everyone, everywhere, working from anywhere,* **was not on the radar screen**. (D2, kursivointi alkup.)

> **COVID-19 amplified everything – In a flash, there was more data to protect** due to unprecedented surge in demand for government services such as unemployment compensation and other digital services, more channels over which that data was traveling, **more threats to deal with**, **more everything –** except funding. (D4b)

> Today's environment is one **not only of heightened risk, but of prolonged uncertainty**. Blurring the lines between business-as-usual risk management, crisis management, and resilience can enable agility in the face of **an uncertain future**. (D5)

Yllättävyyden ja epävarmuuden, joka aineistossa näyttäytyy jatkuvan myös tulevaisuuteen, kautta COVID-19-pandemiasta muodostuu syöte kyberturvallisuuden toimintaympäristön murrokselle. Tällaisissa muuttuneissa olosuhteissa toimiminen edellyttää tilanteen pikaista arviointia ja toimenpiteiden tekemistä siihen sopeutumiseksi. Shokkivaikutuksensa ja epävarmuutensa lisäksi tutkimusaineistossa COVID-19-pandemian nähdään tuoneen näkyväksi organisaatioiden toiminnassa sisällä olleet puutteet sekä lisänneen organisaatioihin kohdistuvia kyberriskejä, erityisesti etätöihin siirtymisen johdosta:

> **COVID-19 has laid bare the vulnerabilities of many organizations**, and accelerated trends that could lead to significant improvements in productivity, performance and resilience, which will enable them to thrive in the "next normal". (D1)

> The COVID-19 pandemic has led to large scale disruption in people's everyday lives, families, communities and businesses. Social distancing has led to fundamental changes in the way organisations operate. **Employees are now working from home where possible** in most countries and connecting to their office networks and systems through the internet. **As a result, the cyber security risks on IT systems** and, importantly, on the SWIFT payment systems **have increased**. (P5)

> The coronavirus (COVID-19) outbreak has caused **an increase in both the likelihood and impact of cyber attacks**, as organisations react rapidly to potentially significant operational and financial challenges. (P9).

Palaan yllä olevassa ensimmäisessä sitaatissa mainittuun "seuraavan normaalin" käsitteeseen vilpittömyyden pätevyysvaatimusta käsittelevässä luvussa

tarkemmin, tässä kohtaa sen sijaan tärkeää on huomion kiinnittäminen COVID-19-pandemian rooliin tutkimusaineistossa kyberriskejä kasvattaneena tapahtumana. Tämä tuodaan esille tarkastelluissa julkaisuissa joko suoraan toteamalla tai implisiittisesti viittaamalla esimerkiksi COVID-19-pandeiaan organisaatioiden haavoittuvuudet valokeilaan tuovana tapahtumana. COVID-19:n uhka- ja riskitasoa organisaatioille nostavana esimerkkinä tutkimusaineiston diskurssissa on se, että kyberrikolliset, hakkerit ja muut pahantahtoiset toimijat tuntuvat viihtyvän huomattavan hyvin uudessa muuttuneessa tilanteessa. Tämä tuodaan aineistossa esille useaan kertaan, esimerkiksi:

> **Hackers and cyber scammers are trying to take advantage of expanding technology footprints and new attack surfaces**, with the most employees working remotely. (D6)

> **COVID-19 also presented new opportunities for criminals** to try and exploit both the public and private sectors, and, as the news media has widely reported, individual citizens have also been increasingly targeted. (D4b)

> We've also seen **an uptick in threat actor activity – they thrive in chaos and the pandemic gives them a wealth of opportunity** to use social engineering to encourage bad clicks and unsafe online activities. (D1)

> While COVID-19 will likely continue to impact businesses for many months, **in the meantime other cyber threats have not dissipated**. It is therefore important to maintain visibility of your entire threat landscape, **as for many cyber criminals or threat actors, it has largely been business as usual**. We have even seen them releasing new tools and widening their targeting across the period. (P2)

> Threat actors are already **exploiting the uncertainty and extraordinary response** caused by the COVID-19 pandemic. (P9).

Täten diskurssissa muodostuu voimakas vastakkainasettelu sekaannuksen ja epävarmuuden keskellä kamppailevien organisaatioiden ja toisaalta juuri tästä sekaannuksista mahdollisuuksia ammentavien rikollisten ja muiden uhkaavien toimijoiden välille. Tämänkaltainen vastakkainasettelu on tyypillistä, mutta myös välttämätöntä turvallisuuspuheelle. Se on lisäksi esimerkki toiseuttamisesta, jossa maailma jakautuu meihin ja meistä eri tavalla toimiviin muihin. Yksi esimerkki tästä on kansainvälisen turvallisuuspolitiikan saralla ollut puhuminen ”sivistyneestä lännestä”, jota uhkaavat ”barbaariset terroristit” (ks. Campbell 1998, 88-89). Tällainen kielenkäyttö sekä rakentaa ja vahvistaa ulkopuolelta tulevaa uhkaa että oikeuttaa vastatoimia tätä toista osapuolta kohtaan. Tutkimusaineistoni kohdalla edellä viitattujen sitaattien kaltainen uhka- ja viholliskuva rakentaa ennen kaikkea tarvetta toimenpiteille, joilla kyberrikollisilla COVID-19-pandemian keskellä oleva etumatka saadaan kurottua umpeen. Tarkastellaan seuraavaksi sitä, mitä tutkimusaineistossa suositellaan muuttuneessa tilanteessa toimimiseksi, pärjäämiseksi ja lisääntyneisiin uhkiin vastaamiseksi.

5.2 Teknologia apuna, mutta myös uusien riskien synnyttäjänä

Tutkimusaineistosta nouseva keskeinen suositus muuttuneessa tilanteessa toimimiseksi COVID-19-pandemian myötä lisääntyneiden riskien hallitsemiseksi on digitaalisiin ratkaisuihin ja teknologioihin panostaminen. Tietoturvayhtiöiden julkaisuissa teknologian olemassaolon nähdään hyödyttäneen organisaatioita myös pandemian alkamisen ja etätöihin siirtymisen keskellä. Tämä viesti online-palveluiden osalta on vahvana Deloitten artikkelissa *New World, New Risk – How COVID-19 is Transforming Business for the Next Normal*:

> The coronavirus pandemic has clearly shown that **the more business functions organizations can perform online, the more resilient they are to disruptive events**. Retail is the most obvious example of this – Amazon and other online powerhouses are thriving during the pandemic, while brick-and-mortar retailers are declining. (D1)

Sitaatissa kuvastuu kahden maailman välinen ero. Siinä missä organisaatioiden ja kyberrikollisten lähtökohdat pandemian keskellä toimimiseen näyttäytyivät edellisessä alaluvussa vastakkaisina, on myös organisaatioiden välillä tutkimusaineistossa eroa siinä, miten nämä muuttuneessa tilanteessa onnistuvat toimimaan: toisella puolella operoivat Amazonin kaltaiset modernit teknologiaa hyödyntävät jättiläiset ja toisella puolella ovat kehityksestä taakse jääneet pienet kivijalkakauppiaat. Tämä uuden ja vanhan maailman ero tulee esille myös siinä, millaista organisaatioiden käytössä olevan teknologian saman artikkelin mukaan tulee olla, tai päinvastoin millaista käytössä olevan teknologian ei ainakaan pidä olla:

> The COVID pandemic has provided **painful lessons on the insufficiency of legacy IT infrastructure at a time when everyone** – employees, customers, partners, etc. – **must interact digitally**. (D1)

Täten tilanteessa pärjäämiseksi tarvitaan nimenomaan uutta teknologiaa, vanhat järjestelmät ja infrastruktuuri, eli niin sanottu ”legacy IT”, ei ole organisaatioille riittävää. Sitaatista kuvastuu myös se, kuinka digitaalisten palveluiden hyödyntäminen ei ole organisaatiolle ainoastaan suotavaa, vaan se on jopa välttämättömyys. Tämä uuden teknologian välttämättömyyden ja tarpeellisuuden diskurssi on läsnä myös useassa muussa tarkastellussa julkaisussa, esimerkiksi:

> **COVID-19 has turned digitization from ”nice to have” to a ”must have”** for many organizations, forcing them to adapt and **modernize quickly** in order to keep their operations running. (D3)

> Over the last few months**, the COVID-19 pandemic has forced many companies to accelerate their digitizaton efforts**. As office closures and restricted movement compelled everyone and everything that could go virtual to do so, many institutions had to more fully embrace a digital transformation in operations, distribution, and customer engagement. (D6)

Cybersecurity organizations will need to quickly adapt to this new operating environment by implementing enhanced controls and endpoint protection technologies **to exert greater control over end-user devices**. (D6)

COVID-19 has forced organisations to rapidly shift to new digital ways of working, with many now using it as a catalyst for permanent changes. (P1)

The COVID-19 crisis has seen a rapid adoption of remote working. **This rapid shift has highlighted the importance of technology investment** in supporting a dispersed workforce or, perhaps, highlighted the need for improvements in that investment. (P6b).

Välttämättömyyden ja pakon lisäksi sitaateista käy ilmi tilanteen ja uuden teknologian kiireellisyys: viitattujen tietoturvayhtiöiden julkaisujen mukaan suositellut toimenpiteet on tehtävä myös nopeasti, koska toimintaympäristö ei ole enää entisensä. Lisäksi PwC:n *2021 Global Digital Trust Insights* -raportissa todetaan suoraan teknologisten innovaatioiden myös tasoittavan vaakakuppeja organisaatioiden puolustuksesta vastaavien ja kyberrikollisten välillä:

Innovation is changing the cybersecurity game, **giving new advantages to defenders and leveling the playing field** with the attackers. (P1b)

Teknologia ei näyttäydy tutkimusaineistossa kuitenkaan ainoastaan suorana oikotienä onneen, vaan siihen koetaan liittyvän myös kääntöpuolensa. Lisämuuttujana teknologian osalta pandemian keskellä turvallisesti toimimisessa toimii tarkasteltujen julkaisujen mukaan nimittäin se, että vaikka organisaatiot digitalisoisivatkin palveluitaan, niin näissä uusissa palveluissa ja teknologioissa sekä niiden käytössä on myös omat riskinsä:

But **with each transformation comes a new set of risks** to consider and mitigate. (D1)

However, **speed of transformation cannot come at the expense of risk**, or the entire initiative can cause more harm than good. It is critical that cybersecurity and other risk factors be considered in the design state of digital transformation initiatives, so the new digitized process does not weaken the overall risk profile of the organization. (D3)

Telecommuting, which increases during public health crisis, **inadvertently can lead to cybercrime**. CISA (Cybersecurity and Infrastructure Security Agency) has just issued an alert regarding vulnerabilities caused by remote access to organizations' computer systems. **A proliferation of cloud-apps makes it easier for bad actors to exploit holes in networks**. (P8)

Täten investoidessaan ja ottaessaan käyttöön uutta teknologia kyetäkseen jatkamaan toimintaansa COVID-19-pandemian keskellä, organisaatiot voivat tietoturvayhtiöiden mukaan altistaa itsensä uusille riskeille. Täten tilanteesta rakentuu kehä, jossa uutta teknologiaa tarvitaan COVID-19-pandemian tuomien riskien kontrolloimiseksi, mutta uuden teknologian myötä avautuu puolestaan uusia riskejä, jotka tarvitsevat omat hallintakeinonsa. Tällainen toimintaympäristö saattaa olla tietoturvateknologioita- ja prosesseja konsultoivalle toimijalle varsin mieleinen.

5.3 Totuusväittämien kautta rakentuva ymmärrys COVID-19-pandemian vaikutuksista kyberturvallisuudelle

Tässä luvussa edellä esiteltyjen tutkimusaineistosta nousseiden havaintojen ja sitaattien perusteella COVID-19-pandemialle muodostuu tietoturvakonsultointiyhtiöiden totuusväittämien kautta selkeä narratiivi. Tässä narratiivissa COVID-19-pandemia on ollut suuri ja ennalta-arvaamaton murros, joka on vienyt organisaatiot uusien kyberriskien täyteiseen epävarmuuden aikaan. Tämän ajan haastavuutta ja uhkaavuutta lisää se, että tällainen epäjärjestys on tarjonnut kyberrikollisille otollisen mahdollisuuksien maaperän, josta harjoittaa toimintaansa. Vastatakseen ajan tuomiin haasteisiin ja tasoittaakseen pelikenttää kyberrikollisiin nähden, tarkastellut tietoturvayhtiöt julkaisuissaan näkevät digitaalisiin palveluihin ja uusiin teknologioihin pikaisen panostamisen välttämättömäksi. Oman lisähaasteensa uusien teknologioiden käyttöönottoon tuo kuitenkin uusien teknologioiden mukanaan tuomat uudet riskit, jotka myös täytyy kyetä huomioimaan ja hallitsemaan.

Täten tarkasteltujen tietoturvayhtiöiden COVID-19-diskurssissa korostuvat kiireellisyyden tuntu, uhkaavammaksi ja vaarallisemmaksi muuttunut toimintaympäristö sekä teknologian rooli näiden haasteiden voittamiseen. Kiireentunnulla voidaan esimerkiksi perustella sitä, miksi organisaatioiden on suunnattava toimenpiteitä tietoturvansa vahvistamiseen välittömästi. Graham & Luke (2011, 111) ovat kutsuneet kiireellistä toimintaa edellyttävien uhkaavien asioiden nostamista julkiseen keskusteluun nykyaikaisen korporatismin tunnuspiirteeksi, koska näihin vetoamalla voidaan perustella yhä suurempaa tarvetta kulutukselle. Tietoturvayhtiöiden viestin kohdalla tämä tarkoittaa suurempaa tarvetta heidän tarjoamilleen palveluille, koska radikaalit ja uhkaavat muutokset organisaatioiden toimintaympäristössä sitä kaipaavat. Teknologian merkityksen painottaminen tutkimusaineistossa on puolestaan osa kyberturvallisuuden diskursseihin liittyvää ”teknillistämistä” (ks. Hansen & Nissenbaum 2009), jolla kyberturvallisuudesta rakentuu nimenomaan teknisten asiantuntijoiden, kuten tietoturvayhtiöiden, toiminta- ja valtakenttää. Tämän edellä kuvatun narratiivin voidaan sanoa olevan tutkimusaineistosta nouseva *sosiaalinen* totuus COVID-19-pandemian vaikutuksista organisaatioiden kyberturvallisuudelle.

Habermasilaisesta diskurssianalyyttisestä kehyksestä käsin totuusväittämien osalta on perinteisesti oltu kiinnostuneita myös siitä, ovatko esitetyt väittämät nimensä mukaisesti perustuneet tosiasioihin. Sosiaalisen konstruktionismin kannalta ajatus jostakin taustalta löytyvästä objektiivisesta totuudesta on ylipäätään ongelmallinen, mutta erityisen ongelmallinen se on COVID-19-pandemian kaltaisen, vielä tutkielman tekohetkellä käynnissä olevan tapahtumasarjan kannalta. Analysoidut tietoturvayhtiöiden julkaisut ovat syntyneet hetkellä, jolloin pandemia on akuutisti ollut käynnissä, eikä vallalla ole ollut mitään yksimielistä

ymmärrystä siitä, mitä tilanteesta parhaiten selviämiseksi tulisi tehdä. Julkaisujen totuusväittämiä ja näiden perusteita tarkastellessa väittämät eivät näyttäydy mitenkään ”epätotuudenmukaisina”. Kuitenkin mielestäni sen selvittämisen sijaan, onko kaikille aineistossa esitetyille väittämille löydettävissä uskottavat lähdeviitteet ja data-aineistot, kiinnostavampaa diskurssianalyyttisestä näkökulmasta on se, millaisia puolia ilmiöstä valitut sanavalinnat korostavat ja millaisia merkityksiä ne tapahtumille tuottavat.

Tästä johtuen huomionarvoista tutkimusaineistosta nousevassa tavassa puhua COVID-19-pandemian vaikutuksista tietoturvallisuudelle on, että se ei ole ainoa mahdollinen tapa kertoa pandemiasta. Esimerkiksi sillä on merkittävä ero, sanotaanko uusiin teknologioihin investoimisen voivan auttaa etätöiden sujuvoittamisessa, vai sanotaanko uusien teknologioiden olevan ”must have”. Lisäksi tilanteen uhkaavuuden kannalta on eroa sillä, nostetaanko esille esimerkiksi ”virkamiesmäisemmin” todettuja COVID-19-aiheisia tietomurtoja, vai todetaanko yleisemmin ja kuvailevammin kyberrikollisuuden ”kukoistavan” lisääntyneiden hyökkäysmahdollisuuksien keskellä.

Käytetty kielenkäyttö tutkimusaineistossa on kuitenkin ymmärrettävää, sillä lisääntyneen kiireellisyyden ja uhkaavuuden korostaminen voi ohjata ja vauhdittaa julkaisujen yleisön päätöksentekoa esimerkiksi uusien tietoturvateknologioiden hankkimisessa. Valittu kielenkäyttö lisäksi noudattaa luvussa 2 kuvatun turvallistamisteorian mukaista turvallistamislogiikkaa, jossa tietoturvayhtiöt pyrkivät nostamaan etätöihin ja puutteellisiin teknologisiin valmiuksiin liittyvät uhat niin korkeiksi, että heidän nykyisten ja potentiaalisten asiakasorganisaatioiden on reagoitava tähän uhkaan, esimerkiksi hankkimalla näiden yhtiöiden tarjoamia palveluita.

Tarkasteltuamme tässä luvussa tietoturvayhtiöiden totuusväittämien kautta muodostuneita merkityksiä ja ymmärrystä COVID-19-pandemiasta organisaatiolle, siirrymme seuraavaksi tarkemmin analysoimaan aineistosta nousevia ja korostuvia tietoturvariskejä ja -suosituksia oikeellisuuden pätevyysvaatimuksen kautta.

6 OIKEELLISUUDEN PÄTEVYYSVAATIMUS

Edellisessä luvussa havaittiin, että tietoturvayhtiöiden julkaisujen kautta COVID-19-pandemia näyttäytyy organisaatiolle kyberturvallisuuden osalta erityisesti etätöihin kiteytyvänä murroksena, jossa pärjääminen edellyttää panostuksia teknologiaan. Tässä oikeellisuuden pätevyysvaatimusta käsittelevässä luvussa puolestaan tarkemmin syvennytään siihen, mitä riskejä, uhkia ja toimenpidesuosituksia julkaisut eniten nostavat esiin. Tämän lisäksi analysoidaan sitä, mihin tahoihin aineistossa viitataan asiantuntijoina ja auktoriteetteina. Täten saadaan selville se, mitä teemoja aineistossa korostetaan ja kenen äänellä siinä puhutaan, eli tosiin sanoen kenen etuja kommunikaatiolla mahdollisesti ajetaan.

Luku jakaantuu kolmeen osaan. Ensimmäisessä osassa tarkastellaan tietoturvariskejä ja -uhkia, joita tietoturvayhtiöt COVID-19-pandemiaan julkaisuissaan liittävät. Toisessa osassa tarkastelu kohdistuu tietoturvayhtiöiden julkaisuissa tekemiin konkreettisiin toimenpidesuosituksiin kyberturvallisuuden parantamiseksi ja ensimmäisessä osiossa mainittujen riskien hallitsemiseksi. Kolmannessa osassa puolestaan analysoidaan sitä, kenen äänellä aineistossa puhutaan ja mitkä tahot aineistossa näyttäytyvät tilannetta koskevina asiantuntijoina.

6.1 Tietoturvariskit ja -uhat COVID-19-pandemian keskellä

Sekä Deloitten että PwC:n julkaisuista yleisimmin esiin nousevat uhat ja riskit COVID-19-pandemian kontekstissa liittyvät etätöiden ominaispiirteisiin sekä etätöiden edellyttämään uuteen ja lisääntyneeseen teknologian käyttöön. Etätöihin siirtymisen johdosta organisaatiolle riskeiksi tutkimusaineistossa ovat muodostuneet esimerkiksi työntekijöiden omat organisaation hallinnan ulkopuolella olevat päätelaitteet (D2), organisaatioiden tekemät priorisoinnit operatiivisen etätyöskentelyn kuntoon saamiseksi turvallisuuskontrollien ja -resursoinnin kustannuksella (D3, P4 & P7), työntekijöiden mahdolliset puutteet kärsivällisyydessä koskien sovittujen työskentelytapojen noudattamista organisaation

prosessien mukaisten työkalujen ollessa poissa käytöstä (P9b) sekä ylipäätään etätöiden avaamat uudet hyökkäysmahdollisuudet ja lisääntynyt hyökkäyspinta (P4 & P5).

Etätöiden synnyttämien riskien lisäksi, ja osittain siihen myös kytkeytyen, toinen läpi tutkimusaineiston toistuva riskiteema on uuden teknologian aiheuttamat riskit. Tietoturvayhtiöiden julkaisujen mukaan digitaalinen transformaatio, jonka vauhtia COVID-19 kiihdyttää (esim. D1 & D3), ja uusien teknologioiden käyttöönotto jo itsessään lisäävät kyberriskejä, sillä uuden teknologian myötä lisääntyy hallittavan ympäristön kompleksisuus sekä samalla vähenee työvoiman osaaminen tämän teknologian käytöstä (D1, D6 & P9b). Lisäksi pilvipalveluiden ja Internetin yli tapahtuvien etäyhteyksien nähdään kasvattavan riskiä, koska tällöin ollaan organisaation perinteisen turvallisuusvyöhykkeen, eli oman konesalin ja sisäverkon ulkopuolella (D6 & P5). Tutkimusaineistossa mukana olevan PwC:n *Global Digital Trust Insights Survey 2021* -raportin mukaan pilvipalveluihin kohdistuvat hyökkäykset koetaan puolestaan kyselytutkimukseen vastanneiden keskuudessa mahdollisilta organisaatioille aiheutuvilta vaikutuksiltaan suurimpina (P1b).

Kuten edellä jo luvussa 6 kävi ilmi, uuden teknologian lisäksi Deloitten julkaisuissa myös vanhojen tietojärjestelmien ja infrastruktuurin (legacy IT) aiheuttamat riskit nousevat aineistosta esille (esim. D1). Käytettävästä teknologiasta riippumaton teknologian ja riskin diskursiivinen suhde ei ole toki vain nyt tarkastelussa olleen tietoturvayhtiöiden COVID-19-diskurssin ominaispiirre, vaan esimerkiksi Wynne (2002, 460) on esittänyt, että riski on kiinteä osa diskurssia, jolla teknologialle ja innovaatiolle julkisessa keskustelussa luodaan merkityksiä. Jantunen & Huhtinen (2011, 8-9) ovat puolestaan havainneet, että yhdysvaltalaisessa poliittisessa diskurssissa kyberin ja uhan käsitteet ovat olleet toisilleen synonyymejä ja esimerkiksi informaatio muuttuu tässä diskurssissa erityisen uhkaavaksi silloin, kun se on verkossa kaikille vapaasti saatavana. Vastaavan kaltaisia teknologian, kyberin, Internetin, riskin ja uhan välisiä ja toisensa yhteen kietovia suhteita on löydettävissä myös analysoimieni tietoturvayhtiöiden COVID-19-diskurssista

Yleisten teknologian käyttöön ja olemassaoloon sekä etätöihin kytkeytyvien riskien ohella aineistosta nousee esille tiettyjä hyökkäystyyppejä, joihin organisaatioiden tutkimusaineistona olleiden tietoturvayhtiöiden julkaisujen mukaan tulee COVID-19-aikana erityisesti varautua. Yleisimmät näistä ovat tietojen kalastelu eli phishing (esim. D2, D4 & P8), kiristys- ja muut haittaohjelmat (esim. D4, P4 & P5) sekä yritykset käyttäjien manipuloimiseksi eli social engineering (esim. D1 & P1b). Näiden hyökkäystyyppien osalta Deloitte esimerkiksi totesi kesäkuussa 2020 julkaistussa *COVID-19 Supercharges Cyber* -artikkelissa uhkatietopalvelunsa toimesta havainneensa pandemian aikana satojatuhansia haittaohjelma- ja tietojen kalastelu -kampanjoita (D2).

Aineistossa organisaatioita uhkaavien toimijoiden osalta eniten puolestaan viitataan rikollisiin toimijoihin (esim. D2, P1b & P5). Esimerkiki PwC kirjoitti tietojen varastamiseen suunnitellun Emotet-haittaohjelman takana olevan rikollisen tahon ryhtyneen käyttämään kalasteluviesteissään COVID-19-pandemiaan

viittaavia sisältöjä (P5). Kyberrikollisten ja muiden edellä mainittujen teemojen lisäksi aineistossa on myös satunnaisia viittauksia esimerkiksi valtiollisiin toimijoihin hyökkäysten taustalla (P4) tai palvelunestohyökkäysten suurempiin haitallisiin vaikutuksiin etätyöaikana (P9b), mutta niiden rooli tarkastellussa diskurssissa on tässä alaluvussa tarkemmin esiteltyjä teemoja vähäisempi.

Tutkimusaineistosta nousseiden riskien ja uhkien esittelyn jälkeen tarkastellaan seuraavaksi niitä tietoturvallisuuden toimenpidesuosituksia, joita aineistosta COVID-19-pandemian ajalle esitetään.

6.2 Tietoturvatoimenpidesuositukset tietoturvallisuuden vahvistamiseksi

Läpi käymässäni aineistossa keskeisimmän perustan toimenpidesuosituksille muodostavat edellisessä luvussa esiteltyjen laajamittaisiin etätöihin siirtymiseen liittyvät riskit. Täten useimmat aineistossa esiin tulleet suositukset liittyvät nimenomaan siihen, miten organisaatioiden tulisi ylläpitää ja kehittää tietoturvaansa etätöiden myötä muuttuneessa toimintaympäristössä. Kaksi keskeisintä aihekokonaisuutta tietoturvasuositusten osalta, jotka aineistosta nousevat esiin, ovat pilvipalveluiden- ja teknologian käyttö (ks. esim. D1, D2 D3, P4, P7 & P9b) sekä identiteetin- ja pääsynhallinta (ks. esim. D2, D4b, D6, P1b, P4, P6 & P6b).

Kuten edellä havaittiin, nähdään tutkimusaineistossa uuden teknologian synnyttävän organisaatioille uusia riskejä, mutta sen lisäksi uusi teknologia, kuten pilvipalvelut, koetaan aineistossa myös mahdollisuudeksi hallita riskejä ja parantaa organisaatioiden tietoturvaa. Pilvipalveluiden osalta niiden käytön nähdään aineistossa parantavan ennen kaikkea palveluiden skaalautuvuutta, joustavuutta, saatavuutta ja vikasietoisuutta (D2, D3 & P9b), jotka saattavat olla pandemian aikana aiempaa suuremmalla koetuksella. Lisäksi pilvipalveluiden nähtiin aineistossa auttavan suojaamaan organisaatioita paremmin myös tilanteissa, joissa etätyöjakso tulisi pitkittymään (P7).

Tutkimusaineistossa identiteetin- ja pääsynhallinnan merkityksen nähtiin kasvaneen, erityisesti korkeita oikeuksia omaavien tunnusten osalta. Identiteetin- ja pääsynhallinta (IAM) on laaja kokonaisuus, jossa yhdistyy niin tietoturvaa, henkilöstöhallinnon prosesseja kuin tietohallinnon ja liiketoiminnan operatiivista tehokkuutta parantamaan pyrkiviä osa-alueita. Identiteetinhallinnan näkökulmasta siihen kuuluvat ensi sijassa prosessit ja teknologiat, joilla hallitaan identiteetin elinkaarta eli esimerkiksi sitä, miten uuden käyttäjän oikeudet provisioidaan kohdejärjestelmään tai miten toimitaan tilanteissa, joissa jo myönnettyjä oikeuksia pitää muuttaa tai poistaa kokonaan. Pääsynhallinnan näkökulmasta ollaan puolestaan kiinnostuneita esimerkiksi siitä, miten tunnistautuminen kohdepalveluihin tapahtuu ja miten näitä pääsyoikeuksia valvotaan. Oman alakokonaisuutensa suuremman IAM-sateenvarjon alle muodostaa pääkäyttäjä- tai muita korkeita oikeuksia omaavien tunnusten hallinta ja tarkempi kontrollointi,

joka tunnetaan englanninkielisellä termillään *Privileged Access Management* (PAM).

Aineistossa etätöiden todettiin hämärtävän entisestään organisaatioiden verkon rajoja, minkä takia fokus tulee siirtää sisä- ja ulkorajan suojaamisesta siihen, että oikeilla henkilöille on pääsy oikeisiin resursseihin. Tästä muutoksesta Deloitte toteaa *The Acceleration of Digitization as a Result of COVID-19* -artikkelissaan, että ”identity has become the new paradigm for enterpise security” sekä ” IAM has become the foundation in the modern secure working environment”(D3). PwC puolestaan omisti identiteetin- ja pääsynhallinnalle kokonaisen white paper -julkaisun otsikolla *Digital Identity supports a secure remote digital workforce during COVID-19*. (P6b). Lisäksi tarve identiteetin- ja pääsynhallintaan panostamiseksi kytkeytyy aineistossa ilmoitettuun kasvaneeseen haittaohjelmien ja kalasteluviestien uhkaan sekä tarpeeseen kyetä suojaamaan organisaatioiden korkeimpia käyttövaltuuksia omaavia tunnuksia (D2). Korkeiden käyttöoikeuksien turvaaminen on ollut esillä tärkeäksi nostettuna osa-alueena jo ennen COVID-19-pandemiaa, sillä esimerkiksi Gartner, vaikutusvaltainen informaatioteknologian tutkimuslaitos, oli listannut kahtena vuotena peräkkäin 2018-2019 juuri korkeiden käyttöoikeuksien hallinnan tärkeimmäksi käynnistettäväksi tietoturvallisuusprojektiksi organisaatioille (Gartner, 2018 & Gartner, 2019).

Pilvipalvelut ja IAM linkittyvät ainestossa myös toisiinsa, sillä Deloitte (D6) näkee pilvipalveluiden yhdessä API-ekosysteemin kanssa lisäävän digitaalisten identiteettien määrää sekä asettavan uusia vaatimuksia tunnistautumiselle. PwC (P6b) puolestaan kehottaa hyödyntämään pilviarkkitehtuuria myös IAM-palveluiden osalta. Yhtenä identiteetin- ja pääsynhallintaan kuuluvana teknologiasuosituksena aineistosta (esim. D3, D4b, P6b & P8) useaan otteeseen nousee suositus monivaiheisen tunnistautumisen (MFA) käytöstä.

Pilvipalveluiden ja identiteetin- ja pääsynhallinnan lisäksi muita suosituksia, jotka nousevat useamman kerran esiin sekä Deloitten että PwC:n julkaisuista, ovat päätelaitteiden hallintaa (esim. D2, D6, P1b & P3) , videoneuvottelu- ja muiden kollaboraatiotyökalujen turvallista käyttöä (esim. D1, P5 & P8) sekä Zero Trust -arkkitehtuurin käyttöönottoa koskevat suositukset (esim. D2, P6b & P8). Zero Trust -arkkitehtuurilla viitataan turvallisuuden malliin, jossa verkon reunojen ja rajojen sijaan keskitytään käyttäjiin, laitteisiin ja resursseihin. Mallin pääideana on se, että millekään käyttäjälle tai laitteelle ei myönnetä pääsyä resurssiin pohjautuen ainoastaan tämän fyysiseen tai loogiseen sijaintiin eli toisin sanoen näiden välillä ei ole mallissa luottosuhdetta. Sen sijaan käyttäjät ja laitteet tunnistetaan ja valtuutetaan aina ennen kuin pääsy resurssiin sallitaan. (Rose et al. 2020). Käytännössä tämä tapahtuu hyödyntämällä esimerkiksi teknologioita, joilla käyttäjän kirjautumis- ja käyttökontekstia valvotaan koko ajan, ja jos tässä havaitaan poikkeamia käyttäjän normaaliin toimintaan (ns. baseline-vertailu), niin pääsy resurssiin evätään. Malli on täten vahvasti sidoksissa edellä esille tulleeseen Deloitten näkemykseen identiteetistä kyberturvallisuuden ”uutena paradigmana”.

Deloitte ja PwC:n julkaisuista löytyy myös eroja siinä, mitä teemoja painotetaan tai ylipäätään nostetaan esille. Deloitten julkaisuissa on vahvempana

suositus ylätasoisemmalle organisaatioiden digitalisoituimiselle (D1, D3 & D4), kun taas PwC:n artikkeleista löytyy yksityiskohtaisemman tason suosituksia esimerkiksi etätyöjärjestelmiin kohdistuvilta palvelunestohyökkäyksiltä (DDoS) suojautumiseksi (P4 & P9b), tietoturvatapahtumien valvonnasta, analysoinnista ja tietoturvavalvomon (SOC) käytöstä (esim. P1b & P5) tai henkilökunnan tietoturvatietoisuuden kasvattamisen ja kouluttamisen tarpeesta (esim. P4 & P8).

Edellä mainittujen teemojen lisäksi tutkimusaineistona olleista Deloitten ja PwC:n julkaisuista löytyi toki myös monia muita yksittäisiä tietoturvasuositusnostoja, mutta tässä luvussa esiin nostetut ovat niitä, jotka aineistossa hallitsivat diskurssia. Yksittäisten nostojen osalta eräs hyvin kiinnostava havainto löytyi PwC:n *COVID-19: Making remote work productive and secure* -artikkelista (P7). Kyseisessä artikkelissa on pitkä lista kysymyksiä, joita organisaation tietoturvasta vastuullisten olisi hyvä pohtia etätyöskentelyn turvallisuuden osalta. Yksi näistä kysymyksistä koski sitä, miten organisaatiot ovat viestineet ja ohjeistaneet työntekijöitään näiden kotona olevien verkkolaitteiden turvallisesta käytöstä. Kysymys on mielenkiintoinen, koska toimiessaan näin organisaatiot tekisivät selkeän rajanylityksen ja perinteisen toimivaltansa laajennuksen pyrkiessään ottamaan myös henkilöstönsä henkilökohtaiset laitteet tietoturvahallintonsa piiriin perustuen COVID-19-pandemian seurauksena voimaantulleisiin etätyöolosuhteisiin.

Tässä alaluvussa esiteltyjen toimenpidesuositusten ja edellisessä luvussa läpi käytyjen riskien ja uhkien jälkeen tarkastellaan seuraavaksi lähemmin sitä, kenen äänellä aineistossa puhutaan ja mihin asiantuntijatahoihin julkaisuissa viitataan.

6.3 Kenen äänellä puhutaan ja kenelle?

Tarkastelluissa tietoturvayhtiöiden julkaisuissa – ehkäpä vähemmän yllättävästi – keskeisimmäksi asiantuntijaääneksi nousevat kyseiset yhtiöt itse. Monissa julkaisuissaan tietoturvayhtiöt vetoavat itse tekemiinsä havaintoihin, kyselytutkimuksiinsa ja omaan asiantuntija-auktoriteettiinsa esittämiensä väitteiden ja näkemysten pohjana (esim. D1, D2, D4b, D6, P1b & P2). Tekemiensä kyselytutkimusten vastaajajoukkona on puolestaan toiminut ensi sijassa vastanneiden organisaatioiden tietoturvapäälliköt ja tietohallintojohtajat, mutta tiettyjen asiakokonaisuuksien osalta myös muu niin sanottu C-porras, eli esimerkiksi toimitus- ja talousjohtajat. Tarkastellusta aineistosta löytyy viittauksia myös kolmansiin osapuoliin, kuten uutissivustoihin (D3, P7 & P8), kansallisiin viranomaisiin (P5 & P7), tietoturvateknologioita tuottaviin tietoturvayhtiöihin (P8) sekä standardointiorganisaatioihin (P2 & P8).

Tarkastellun tutkimusaineiston keskustelijaosapuolista havaitaan, että kyse on osallistujiltaan tarkkaan rajatusta joukosta. Kyse on ennen kaikkea tietoturvayhtiöiden oman asiantuntijatiedon ja -äänen jakamisesta yleisönä toimiville organisaatioiden tietoturvasta vastaaville toimijoille, joiden ääni puolestaan pääsee aineistossa osittain kuuluville tietoturvayhtiöiden heille tuottamien kyselytutkimusten kautta.

Stahl et al. (2012) Iso-Britannian terveydenhuollon tietoturvapolitiikkoja analysoidessaan havaitsivat, että niissä keskeisenä auktoriteettina toimivat organisaatioiden johto ja tekniset asiantuntijat, joiden sanomisia ja tahtoa politiikat määräävät organisaatioiden muun henkilökunnan noudattamaan. Vastaavan kaltainen valta-asetelma on löydettävissä myös nyt analysoiduista tietoturvayhtiöiden julkaisuista. Varsinainen loppukäyttäjäkunta ei ole dialogissa mukana, vaan he ovat julkaisujen diskurssissa ennemminkin etätyömaailmaan ajauduttuaan uusien teknologioiden keskellä riskien lähde ja tietoturvakonsultointiyhtiöiden antamien toimenpidesuositusten sekä niitä toteuttavien organisaatioiden tietoturvapäättäjien toiminnan kohde.

Oikeellisuuden pätevyysvaatimusta vasten arvioituna voidaan täten todeta, että organisaatioiden henkilökunta ja loppukäyttäjät eivät ole kommunikaatiossa mukana oman äänen omaavana toimijana, vaan julkaisut tuottavat osaltaan valta-asetelmaa, jossa tieto- ja kyberturvallisuus ovat asiantuntijakonsulttien ja organisaatioiden tietohallintojohdon määrittelemää pelikenttää. Tämä puolestaan johtaa siihen, että näiden kyberturvallisuuspuheen kannalta valta-asemassa olevien toimijoiden näkemykset ja kannanotot muodostavat kyberturvallisuudesta totuuksia, joiden haastaminen ja kyseenalaistaminen näiden ryhmien ulkopuolelta on vaikeaa.

7 VILPITTÖMYYDEN JA YMMÄRRETTÄVYYDEN PÄTEVYYSVAATIMUKSET

Pro gradu -tutkielmani viimeisessä tutkimusaineiston analyysia koskevassa luvussa perehdytään aineistoon kommunikaation vilpittömyyden ja ymmärrettävyyden pätevyysvaatimusten kautta. Vilpittömyyden kohdalla aineistosta analysoidaan siinä käytettyjä adjektiiveja, vertauskuvia ja sanojen konnotaatioita, sekä pohditaan sitä, kuinka nämä mahdollisesti ohjaavat ymmärrystä COVID-19-pandemian merkityksestä kyberturvallisuudelle johonkin tiettyyn suuntaan. Ymmärrettävyyden osalta puolestaan keskitytään ylipäätään siihen, kuinka nimensä mukaisesti ymmärrettävää käytetty kieli on, sisältääkö se esimerkiksi teknistä jargonia tai muita epäselviä termejä ilman selityksiä, jotka myös vaikuttavat ja ohjaavat julkaisuiden lukijoiden ymmärrystä aiheesta.

7.1 Tietoturvayhtiöiden julkaisujen vilpittömyys

7.1.1 Tilanteen uhkaavuuden korostaminen

Vilpittömyyden pätevyysvaatimuksen osalta tietoturvayhtiöiden julkaisuista tarkastelun perusteella nouseva yleiskuva on se, että aineistossa ei ole havaittavissa räikeitä julkaisujen lukijoiden harhaanjohtamisen pyrkimyksiä. Kuitenkin, kuten aiemmissa totuuden ja oikeellisuuden pätevyysvaatimuksia käsitelleissä luvuissa 6 ja 7 havaittiin, korostuvat diskurssissa tietyt näkökulmat ja piirteet toisten kustannuksella, jotka osaltaan vaikuttavat myös julkaisujen vilpittömyyteen ja rehellisyyteen.

Luvun 6 mukaisesti julkaisujen tuottamassa COVID-19-päänarratiivissa organisaatiot ovat ajautuneet epävarmuuden ja murroksen keskelle, johon kyberturvallisuuden kannalta lisähaasteensa tuovat sofistikoituneet ja epäjärjestyksen keskellä kukoistavat kyberrikolliset. Epävarmuutta, epäjärjestystä ja kyberrikollisten kyvykkyyttä vallitsevien olosuhteiden keskellä korostavien ilmaisujen

kautta korostuu myös tilanteeseen liittyvä vaaran, turvattomuuden ja niiden ratkaisemiseksi tarvittavien nopeiden päätösten tarpeen tuntu. Vaaran, uhan ja epävarmuuden korostamisen osalta pohdittavaksi jää, korostetaanko näitä puolia tapahtumista sen takia, että julkaisuiden lukijat suhtautuisivat riittävällä vakavuudella COVID-19-pandemian seurauksiin myös kyberturvallisuuden osalta vaiko kenties siksi, että tällainen kielenkäyttö mahdollisesti vauhdittaa tietoturvayhtiöiden omaa liiketoimintaa?

Pelolla markkinointi on ollut perinteinen tapa turvallisuusaloilla oman agendan edistämiseksi. Tästä esimerkiksi Chris Krebs, Yhdysvaltojen kyberturvallisuusviranomaisen CISA:n entinen johtaja, on todennut, että kyberturvallisuustoimijoiden tulisi viestinnässään kyetä pelonlietsontaa ja hysterisointia parempaan (O'Gara 2019). COVID-19-pandemian kaltainen tilanne siihen kytkeytyvien terveysuhkien myötä on monille jo valmiiksi pelon ja huolen täyttämä. Tämä uhkaavuuden "kivijalka" puolestaan tarjoaa mahdollisuuden pelon siirtämisen ja rinnastamisen myös kyberturvallisuuden puolelle. PwC:n julkaisussa *How to protect your companies from rising cyber attacks and fraud amid the COVID-19 outbreak* COVID-19-viruksen ja tietoturvauhkien leviäminen rinnastetaan seuraavasti:

> **Social engineering campaigns** that preyd upon fear over the virus began appearing in late January and **have spread as quickly as the disease**. Malicious actors typically pose as a trusted organization (banks, merchants) or individual (co-worker, manager, IT adminsitrator). **The volume of malicious email has rocketed**, according to Proofpoint, a cybersecurity company monitoring virus-related cybercrime. (P8)

Täten COVID-19-pandemian kohdalla digitaalisiin palveluihin nojaaville organisaatioille uhka on kaksinkertainen, kun työntekijöiden terveyden perässä olevien biologisten virusten vanavedessä samaa tahtia seuraavat digitaaliset virukset ja uhat. Tilanteen korostunut uhkaavuus ei näyttäydy tutkimusaineistossa kuitenkaan aina pelkästään negatiiviseksi ja riskienhallintaa edellyttäväksi asiaksi, vaan Deloitten käyttämässä retoriikassa COVID-19:n myötä organisaatioissa on myös "kiihtynyt" moni asia, kuten pilvipalveluiden käyttö sekä yleinen tietoisuuden kasvu kyberturvallisuuden merkityksestä:

> **COVID-19 has already caused acceleration in several cyber related areas**. […] many organizations accelerated their journey to the cloud when remote-work policies came into effect. (D2)

> Of all the accelerations caused by COVID-19, **the most important could be the acceleration of people's understanding of the impact of cyber**. (D2)

Tällaisessa kontekstissa käytettynä kiihtyminen sanana pitää sisällään ennen kaikkea myönteisiä ja organisaatioiden toimintaa mahdollistavia sekä eteenpäin vieviä konnotaatioita. Näin ollen COVID-19-pandemian myötä lisääntyneiden uhkien korostaminen ei ole pelkkää pelolla ratsastamista, vaan nämä uhat ovat myös mahdollisuuksia organisaatioille toimintansa kehittämiseen kyberturvallisuuden osalta.

7.1.2 Kohti seuraavaa normaalia

Kielikuvien osalta Deloitten julkaisuissa useaan otteeseen käytetty tilannetta voimakkaasti kuvaava ilmaisu on ”the next normal” (D1, D2 & D3). ”Seuraavan” tai ”uuden” normaalin käsite COVID-19-pandemian yhteydessä on varmasti tuttu ilmaisu meistä useimmille, ehkä jopa kyllästymiseen asti, sillä niin paljon näitä termejä on käytetty esimerkiksi päättäjien ja tiedotusvälineiden toimesta kuin myös tuttavien kesken kahvipöytäkeskusteluissa. Deloitten julkaisuissa ”seuraava normaali” kytkeytyy tietoturvan kannalta erityisesti etätöihin, mutta myös tarpeeseen osata toimia näissä muuttuneissa olosuhteissa:

> **The world is going to look different in the next normal** due to the COVID-driven acceleration of existing trends – **work from home**, social responsibility, sustainability, and so on. (D1)

> **Cyber teams will need to understand how organizations will function in the post-COVID ”next-normal”**. They need to take stock of all of the business processes they need to support, and rethink what cyber resilience really means. Once that’s done, they **can reevaluate security architectures and operations to map to their digital footprint in the next normal**. (D2)

> Finally, **to thrive in the Next Normal**, organizations should consider **conducting risk assessments** of digitized processes and take appropriate actions to **remediate any identified security gaps**. (D3)

Asonye (2020) on todennut ”uusi normaali” -ilmaisun luovan vahvaa kuvaa uudesta maailmanjärjestyksestä, josta ei enää ole paluuta vanhaan. Tietoturvayhtiöiden julkaisuissa tämä kielikuva viestittää myös sitä, että organisaatiolla aiemmin hallussa olleet teknologiat, prosessit ja muut kyvykkyydet eivät ole enää riittäviä, vaan niiden tilalle tarvitaan uutta, joka toimii COVID-19-pandemian myötä alkaneessa uudessa ja sitä seuraavassa normaalissa. COVID-19-pandemian vaikutukset eivät näin ollen ole analysoidussa diskurssissa vain hetkellinen murros, vaan niitä seuraa perustavaa laatua oleva muutos organisaatioiden digitaaliselle toiminnalle ja sen turvaamiselle.

Normaalin ja normaaliuden käsitteet ovat erittäin voimakkaita, sillä niiden vastakohtana on aina jokin, mikä on epänormaalia. Luokittelu normaalin ja epänormaalin kategorioihin on vallankäyttöä, joka ovat länsimaisissa yhteiskunnissa olleet voimakkaasti esillä esimerkiksi vankeinhoidossa ja seksuaalista suuntautumista koskevissa kysymyksissä (ks. Foucault 1980 & 2010). Toisin sanoen, jos toiminta ei ole yhteiskunnan määrittelemien normien mukaista, on se kiellettyä, tuomittavaa tai vähintäänkin leimauttavaa, ja tällaista harva toimintansa todennäköisesti haluaa olevan. Niinpä normaalin käsitteeseen yhdistyy vahvasti sisäänkirjoitettuja sääntöjä siitä, miten yksilön tai yhteisön tulee toimia. Eli jos COVID-19 on tuonut mukanaan uuden normaalin organisaatioiden tietohallinnoille ja tietoturvalle, täytyy näiden organisaatioiden toimia sen mukaisesti ollakseen ”normaaleja”.

Uuden tai seuraavan normaalin käsitteet muuttuvat vaarallisiksi silloin, kun niiden kautta ryhdytään oikeuttamaan poikkeusaikana voimaan tulleita toimia myös tämän päättymisen jälkeen. Se mikä oli ennen ymmärretty poikkeustilaksi, muuttuukin ”uuden normaalin” myötä olosuhteiksi, miten asioiden tuleekin olla. Kyberturvallisuuden kohdalla panostukset esimerkiksi pilvipalveluihin tai identiteetinhallintaan eivät vielä itsessään uhkaa laajamittaisesti yksilönvapauksia tai ihmisoikeuksia, mutta COVID-19-pandemian myötä esimerkiksi kasvanut terveystietojen käsittely ja jakaminen sekä ihmisten liikkumisen valvonta ja näiden normalisoituminen voivat sitä jo tehdä (ks. Timotijevic 2020).

Asonye (2020) on lisäksi huomauttanut, että puhuttaessa ”uudesta normaalista” suhteessa COVID-19-pandemiaan ja digitaalisiin palveluihin, suljetaan samalla tämän normaalin ulkopuolelle se toinen puoli maapallon väestöstä, jolla ei ole tällä hetkellä pääsyä Internetiin. Täten etätyöt ja niiden normalisoiminen ovat osaltaan myös vallankäyttöä ja nimenomaan puhetta hyväosaisille, heille, joilla ylipäätään on mahdollisuus käyttää digitaalisia ja verkottuneita palveluita. Tietoturvayhtiöt ja heidän yleisönään olevat organisaatiot kuuluvat tähän hyväosaisten joukkoon, ja tämä puoli kyberturvallisuudesta keskusteltaessa usein unohtuu: puhe kyberturvallisuudesta on ennen kaikkea puhetta niiltä niille, joilla on jo kaikkea.

7.2 Julkaisujen ymmärrettävyys

Tutkimusaineistona olleiden tietoturvayhtiöiden julkaisujen ymmärrettävyyttä koskien tarkastelu kohdistui näiden käyttämän kielen selkeyteen, teknisen jargonin määrään sekä mahdollisen muuten epäselvän ja vaikeasti ymmärrettävän terminologian käyttöön.

7.2.1 Tekninen jargon

Yleishavaintona julkaisuista voidaan todeta, että kielenkäytön osalta lauserakenteet ja julkaisujen sisällön yleinen ymmärrettävyys ja selkeys ovat hyvällä tasolla. Teknisen jargonin osalta julkaisut ovat sitä täynnä, mikä ei tietoturvakonsultointiyrityksistä ollessa kyse ole yllätys, ja termit kuten VPN, Zero Trust, phishing ja ransomware toistuvat lähes julkaisusta toiseen. Huomioiden julkaisujen yleisön, eli tietoturvasta asiakasorganisaatioissa vastaavat tahot, tämänkaltaisen jargonin käytön ei pitäisi vaarantaa kohdeyleisön kykyä ymmärtää lukemaansa.

Julkaisuissa käytetyt tekniset termit ja lyhenteet ovat olleet kyberturvallisuutta koskevassa keskustelussa esillä jo näitä julkaisuja aiemminkin, lukuun ottamatta PwC:n julkaisusta *How to protect your companies from rising cyber attacks and fraud amid the COVID-19 outbreak* löytynyttä termiä ”Borderless Data Access Control (BDAC)” (P8), jolla viitattiin pääsynhallintaan hybridiympäristössä, jossa selvä sisä- ja ulkorajaa organisaation verkolle ei ole enää olemassa.

Kyseisestä termistä ei Googlella tehdyn haun perusteella löytynyt muita suoraan vastaavia mainintoja, joten kyseessä on mahdollisesti termi, jota PwC ja muut toimijat ovat vasta pyrkimässä nostamaan osaksi kyberturvallisuudesta käytävää keskustelua. Tämä on myös osoitus vallankäytöstä tai ainakin pyrkimyksestä siihen, koska sillä kenen lanseeraamilla ja määrittelemillä termeillä keskustelua käydään, on puolestaan vaikutusta siihen, kenen etuja keskustelussa ajetaan. BDAC:n kaltaisten uusien teknisten termien keskusteluun nostamisen merkitys tietoturvayhtiöiden palveluiden myynnin, asiantuntijaprofiilin ja heidän asiakkaiden kiinnostuksen nostattamisen kannalta olisi myös oma mielenkiintoinen tutkimuskysymyksensä, mutta siihen ei tässä tutkielmassa kuitenkaan tämän enempää mennä.

Huomioitavaa teknisen jargonin käytön osalta on se, että vaikka tällainen jargon onkin todennäköisesti ymmärrettävää julkaisuiden tavoitellun kohdeyleisön kannalta, on jargonin käyttö kuitenkin myös vallankäyttöä, jolla kyberturvallisuuden kontekstissa tuotetaan ja ylläpidetään jo olemassa olevia sosiaalisia valtasuhteita, joissa kyberturvallisuus on aihealueena teknisten asiantuntijoiden kenttää (Stahl et al. 2012, 86; ks, myös Hansen & Nissenbaum 2009). Analysoidut tietoturvayhtiöiden julkaisut ovat osaltaan tuottamassa tätä suhdetta, sillä tietoturva-asiantuntijoiden ja -tutkijoiden sekä muiden alaan tekniseltä kannalta perehtyneiden ulkopuolisille henkilöille julkaisujen sisältämä kieli ja merkitykset jäisivät epäselväksi.

7.2.2 Määrittelemätön digitalisoituminen

Epäselväksi ja auki selittämättä jäävien käsitteiden osalta Deloitten julkaisuissa ”digitalisoituminen” on osittain tällainen kattokäsite. Aineistossa digitalisoitumisen ja siihen pyrkimisen annetaan ymmärtää olevan COVID-19 myötä muuttuneissa olosuhteissa vaatimus ja pakollinen kyvykkyys organisaatioiden toiminnan menestyksekkäälle jatkumiselle (D1, D3 & D6). Digitalisoituminen kiinnittyy aineistossa erityisesti etätöiden tukemiseen, kuten kollaboraatiotyökalujen ja pilvipalveluiden käyttöön. Pilvipalveluista esimerkkinä digitalisoitumisesta todetaan Deloitten *Covid-19 Supercharges Cyber* -julkaisussa seuraavasti:

> […] while there was a healthy pace of cloud migration prior the pandemic, many organization accelerated their journey to the cloud when remote-work policies came into effect. (D2)

Sitaatissa mainitaan pilveen siirtymisen ”terve” nopeus, mutta sitä mitä tällä konkreettisesti tarkoitetaan tai mikä on tämä siirtymän päätepiste, ei julkaisussa tarkemmin avata. Kysymyksen voisi pukea myös niin, että mikä on riittävä määrä pilvisiirtymää tai digitalisoitumista ylipäätään, ja milloin digitalisoituminen on valmista? Tähän aineistossa ei ole vastausta, vaan digitalisoituminen on samalla sekä keino että päämäärä itsessään, jonka tarkkaa sisältöä ei ole tiedossa. Toisin sanoen digitalisoituminen on tavallaan arvo, kuten esimerkiksi onnellisuus, jota tulee pyrkiä tavoittelemaan koko ajan lisää, pohtimatta liikaa sitä, mikä

on riittävä määrä digitalisoitumista tai onnellisuutta. Täten digitalisoitumisen kaltaiset käsitteet on hyvä pitääkin osin epäselvinä, jos tarkoituksena on tarjota palveluita käsitteen ympärille, koska tämä antaa mahdollisuuden käsitteen uudelleenkäyttöön aina tarpeen ja kontekstin mukaan.

8 TULOKSET JA JOHTOPÄÄTÖKSET

Pro gradu -tutkielmassani olen analysoinut tietoturvayhtiöiden COVID-19-diskurssia kahden monikansallisen tietoturvakonsultointiyhtiön, Deloitten ja PwC :n, kotisivuillaan julkaisemien artikkelien, blogien ja raporttien kautta. Tässä luvussa käydään yhteenvetomaisesti läpi tämän analyysin tuloksena syntyneet löydökset ja johtopäätökset niiden pohjalta. Lisäksi luku sisältää katsauksen tutkimuksen rajoitteisiin ja onnistumiseen, siihen mikä meni hyvin ja mitä puolestaan olisi voinut tehdä mahdollisesti toisin. Luvun lopuksi pohdin mahdollisia jatkotutkimuskohteita, joihin tutkielmani tematiikan ympäriltä tutkimusta voisi laajentaa.

8.1 Tutkielman tulokset

Pro gradu -tutkielmani päätutkimuskysymyksinä olivat 1) millaiseksi COVID-19-pandemian merkitys ja vaikutus organisaatioiden kyberturvallisuudelle tutkimusaineistossa kuvataan, 2) mitä mahdollisia seurauksia ja vaikutuksia tutkimusaineiston kielenkäytöllä on ymmärryksellemme kyberturvallisuudesta COVID-19-pandemian aikana ja 3) Millaisia kyberturvallisuuteen liittyviä valtasuhteita julkaisut tuottavat ja ylläpitävät? Vastaukset näihin kysymyksiin haettiin analysoimalla yhteensä 19 kappaletta Deloitten ja PwC:n julkisesti saatavilla olevia COVID-19-aiheisia tietoturva-artikkeleita, -blogikirjoituksia ja -raportteja. Analyysi tehtiin noudattamalla habermasilaisen diskurssianalyysin menetelmiä, joissa aineisto analysoitiin vasten neljää Jürgen Habermasin määrittelemää kommunikaation pätevyysvaatimusta, jotka ovat totuus, oikeellisuus, vilpittömyys ja ymmärrettävyys.

Diskurssianalyysin tuloksena havaittiin, että COVID-19-pandemia näyttäytyy tutkimusaineistossa ennen kaikkea suurena ja ennalta-arvaamattomana murroksena, joka koskettaa myös organisaatioiden kyberturvallisuutta. COVID-19 on lisäksi lisännyt diskurssissa organisaatioihin kohdistuvia kyberriskejä

merkittävästi. Aineistossa korostui lisäksi vastakkainasettelu COVID-19-pandemian mukanaan tuoman epävarmuuden kanssa kipuilevien ja kamppailevien organisaatioiden sekä puolestaan tämän epävarmuuden ja kaaoksen keskellä kukoistavien kyberrikollisten välillä. Riskien osalta aineistossa korostuivat erityisesti etätöihin ja sen toteuttamiseen tarvittaviin uusiin teknologioihin liittyvät riskit, joita kyberrikolliset voivat käyttää hyväkseen. Vaikka uusiin teknologioihin nähtiin aineistossa liittyvän riskejä, uusien teknologioiden käyttöönottoon myös kannustettiin sekä pelikentän tasoittamiseksi kyberrikollisiin nähden että myös ylipäätään COVID-19-tilanteen myötä muuttuneessa toimintaympäristössä pärjäämiseksi. Uutta teknologiaa tarvitaan tietoturvayhtiöiden aineiston mukaan myös siksi, että vanha "legacy IT" on riittämätöntä COVID-19-pandemian jälkeisessä maailmassa toimimiseksi. Teknologialla on aineistossa siten kaksoisrooli, se sekä synnyttää tietoturvariskejä että toimii näiden riskien paikkaajana. Uuden tietoturvateknologian osalta aineistossa korostuivat erityisesti pilvipalveluihin sekä identiteetin- ja pääsynhallintaan liittyvien teknologioiden tärkeys COVID-19-pandemian aikaisessa ja sen jälkeisessä maailmassa.

Habermasin kommunikaation pätevyysvaatimusten kautta luokiteltuna ja arvioituna COVID-19-pandemia kyberturvallisuuteen kohdistuvana riskejä kasvattavana murroksena on aineiston keskeisin totuusväittämä. Oikeellisuuden osalta puolestaan aineistossa riskien ja toimenpidesuositusten osalta korostuivat edellä mainitut etätyöt, niiden tarvitsemat uudet teknologiat sekä pilvipalveluihin ja IAM-teknologioihin ja -prosesseihin liittyvät panostamissuositukset. Tarkasteltujen julkaisujen vilpittömyyden osalta havaittiin, että kieli on monin paikoin hyvin kuvailevaa, jonka kautta vahvistuu COVID-19-pandemiaan liittyvä vaaran ja turvattomuuden tunne myös kyberturvallisuuden osalta. Voimakkaimpana tilannetta ja sen jälkiseurauksia kuvaavana ilmaisuna käytettiin "seuraavan normaalin" käsitettä. Ymmärrettävyyden pätevyysvaatimuksen osalta puolestaan huomattiin, että julkaisut sisältävät paljon tietoturvateknistä jargonia, mutta tämä ei välttämättä vaaranna tekstien ymmärrettävyyttä, sillä julkaisut ovat lähtökohtaisesti suunnattu tietoturvasta tietoisille ja sen osalta päätöksiä tekevälle yleisölle. Yksittäisten epäselvien termien osalta havaittiin, että "digitalisoituminen" on termi, jonka sisältöä ei tarkasti käytön yhteydessä määritellä. Toisaalta digitalisoituminen nähdään osassa aineistoa COVID-19-pandemian myötä organisaatioille välttämättömäksi, mutta toisaalta digitalisoitumissuosituksia lukevalle yleisölle ei määritellä mikä on riittävä määrä digitalisoitumista tai milloin organisaatiot ovat tämän suhteen valmiita.

Habermasilaisessa diskurssianalyysissa on aiemmassa tutkimuksessa oltu kiinnostuneita kommunikatiivisista häiriöistä, jotka vievät kommunikaatiota kauemmas kaikille osapuolille tasa-arvoisesta ideaalista puhetilanteesta. Tällaisia häiriöitä ovat esimerkiksi perusteettomien totuusväittämien esittäminen, tiettyjen puolten häivyttäminen keskustelusta tai toisaalta joidenkin asioiden korostaminen ja tätä puolta asiasta vahvistavien adjektiivien käyttö. Tutkimusaineistostani tehtyjä löydöksiä, kuten puhuminen "seuraavasta normaalista" tai liittämällä kyberrikollisiin kuvauksia kuten "sofistikoituneet " tai kaaoksen keskellä "kukoistavat", voidaan pitää tällaisina häiriöinä, sillä ne painottavat tilanteen

murrosmaisuutta ja vaarallisuutta. Vastavuoroisesti voitaisiin nimittäin sanoa myös, että COVID-19-pandemia on organisaatioille hetkellinen katkos pysyvän muutoksen sijaan, tai että kyberrikollisten käyttämät menetelmät pandemian keskellä ovat vanhoja tuttuja, mutta ne on vain puettu pandemian myötä uusiin vaatteisiin. Lisäksi tietoturvan kehittämiseksi tutkimusaineistossa tehdyistä useista suosituksista huolimatta aineistossa ei kertaakaan tuoda esille, mitä nämä kehitystoimenpiteet, jotka monissa tapauksissa edellyttäisivät investointeja, tulisivat maksamaan.

Mielestäni ideaalista puhetilanteesta kauemmaksi ajautumista kiinnostavampaa kommunikatiivisten häiriöiden kohdalla on se, että ne tuovat esiin vallitsevia kyseenalaistamattomia totuuksia asioiden tilasta, eli ideologioita, tai vähintäänkin pyrkimyksiä tällaisten ideologioiden tuottamiseksi. Näihin ideologisiin totuuksiin liittyy aina vallankäyttöä, sille sen etuja tilanne palvelee, kenen totuuden mukaan tilannetta tulkitaan ja ymmärretään. Tutkimusaineiston tuottama keskeinen totuus on COVID-19-pandemian kyberturvallisuudelle lisäämät riskit ja vaarallisuuden tuntu, jota voidaan hallita kyberturvallisuuteen tehtävillä teknologia- ja prosessi-investoinneilla. Lisäksi tutkimusaineistossa kommunikaatio rajautuu asiantuntijakonsulttien sekä organisaatioissa tietoturvan osalta päätäntävaltaa pitävien, eli yritysten johdon ja tietoturva-asiantuntijoiden, väliseksi kanssakäymiseksi. Niin sanottujen tavallisten työntekijöiden ääni ei keskustelussa pääse esille muuten, kuin esimerkkinä riskejä lisäävästä toimijasta.

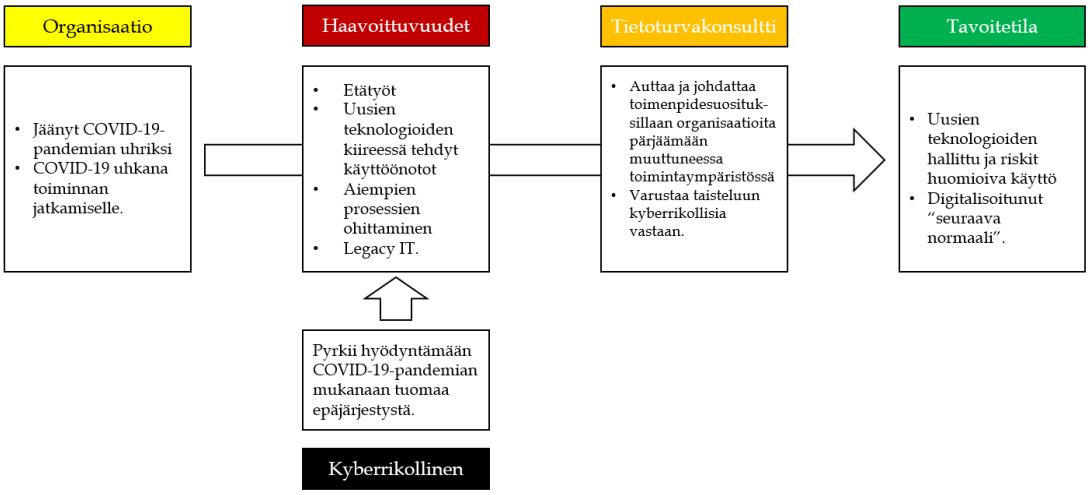
Ideologian, jossa vallalla on jaettu ymmärrys COVID-19-pandemian myötä tulleesta pikaisesta tarpeesta teknologiainvestoinneille sekä käsitys tietoturvakonsulteista auktoriteetin omaavina tahoina näitä suosituksia antamaan, on helppo nähdä edesauttavan ainakin näiden teknologioiden ympärille palveluita tarjoavien konsulttien asemaa kyberturvallisuuden kentällä. Analysoitujen tietoturvayhtiöiden COVID-19-diskurssissa tietoturvakonsultit näyttäytyvät täten pelastajina ja oppaina, jotka johdattavat COVID-19-kurimuksen keskellä olevat organisaatiot toimenpidesuosituksillaan seuraavan normaalin aikakauteen ja varustavat organisaatiot tarvittavilla aseilla taisteluun kaaoksesta voimansa saavia kyberrikollisia vastaan. Analysoidut tietoturvayhtiöt eivät eksplisiittisesti korosta asemaansa COVID-19-diskurssin sankareina, mutta kun otetaan huomioon diskurssissa organisaatioiden lähtötilanne, eli COVID-19-pandemian myötä tullut kriisi ja kasvaneet tietoturvauhat, sekä kenen neuvoilla tästä tilanteesta selvitään, niin havaitaan, että tämä rooli kertomuksessa konsulteille kuitenkin lankeaa, mikä ei välttämättä ole täysin sattumaa.

Tiivistelmä tutkimuskysymyksistä ja niihin tehdyistä löydöksistä löytyy taulukosta 3. Kuviossa 2 on puolestaan esitetty analysoidun COVID-19-diskurssin eri toimijoiden roolit.

Tutkimuskysymys	**Tehdyt havainnot**
Millaiseksi COVID-19-pandemian merkitys ja vaikutus organisaatioiden kyberturvallisuudelle tutkimusaineistossa kuvataan?	• COVID-19-pandemia on organisaatioiden kyberturvallisuudelle murros, joka on lisännyt riskejä ja uhkaavuutta ja

	edellyttää tietoturvainvestointeja sekä digitalisoitumista • COVID-19 on vienyt organisaatiot epävarmuuden keskelle, mutta kyberrikolliset sitä vastoin nauttivat tällaisessa ympäristössä toimimisesta • Etätyöt ja uudet teknologiat koetaan suurimmiksi riskejä lisääviksi osa-alueiksi • Toimenpidesuosituksissa korostuvat pilvipalveluiden ja identiteetin- ja pääsynhallinnan rooli. • Organisaatiot tarvitsevat tietoturvakonsultteja johdattavamaan organisaatiot COVID-19-kyberkriisistä toimenpidesuosituksillaan seuraavaan normaaliin.
Mitä mahdollisia seurauksia ja vaikutuksia julkaisujen kielenkäytöllä on ymmärryksellemme kyberturvallisuudesta COVID-19-pandemian aikana?	• COVID-19-pandemia edellyttää organisaatioilta investointeja kyberturvallisuuteen (teknologiat ja konsultointipalvelut), koska riskit ovat kasvaneet ja "seuraavassa normaalissa" organisaatioiden vanhat teknologiat ja prosessit eivät tietoturvakonsulttien mukaan ole riittäviä.
Millaisia kyberturvallisuuteen liittyviä valtasuhteita julkaisut tuottavat ja ylläpitävät?	• Kyberturvallisuus on tietoturva-asiantuntijoiden ja -konsulttien sekä organisaatioissa näistä asioista vastaavien toiminta-aluetta.

Taulukko 3. Tiivistelmä tutkimustuloksista.



Kuvio 2. COVID-19-diskurssin toimijat.

8.2 Tutkielman rajoitteet

Pro gradu -tutkielman tutkimustulosten esittelyn jälkeen on paikallaan käydä mietteitäni ylipäätään tutkimusprosessin onnistumisesta, rajoitteista ja siitä mitä olisi voinut mahdollisesti tehdä toisin. Lähtökohtana tutkielman tekemiselle ja tutkimusaiheen valinnalle itselleni oli se, että tekisin työn, jossa hyödynnettäisiin konstruktionistisia ja diskurssianalyyttisia tutkimusmenetelmiä. Näin siksi, että tietoturvakeskustelussa sosiaalisen toiminnan rooli on jäänyt valitettavan vähäiselle. Ihminen näyttäytyy keskusteluissa ”heikoimpana lenkkinä” (loppukäyttäjät), huijattavana (social engineering) tai organisaatioiden tarvitsemana osaamiskompetenssina (tietoturva-ammattilaiset), mutta se miten ihmisten välinen vuorovaikutus ylipäätään tuottaa ja muokkaa käsityksiämme kyberturvallisuudesta ja sen tarpeesta, jää hyvin monesti purkamatta ja problematisoimatta. Selaillessani aiemmin kyberturvallisuuden oppiaineeseen Jyväskylässä tehtyjä pro graduja, huomasin että tällaista tutkimusta ei myöskään Jyväskylässä oppiaineen sisällä juurikaan ollut tehty. Tutkimusmenetelmän tarkka rajautuminen nimenomaan habermasilaiseen diskurssianalyysiin puolestaan seurasi siitä, että kyseistä menetelmää oli tietojärjestelmätieteiden ja myös tietoturvallisuuden tutkimuksen kohdalla aiemmin hyödynnetty löytämieni kansainvälisten tutkimusartikkeleiden perusteella. Malli menetelmän hyödyntämiseen tutkimusalan sisällä oli näin ollen olemassa.

Tutkielmani suurimpana ansiona pidän juurikin oppiaineessa harvemmin hyödynnetyn konstruktionistisen lähestymistavan hyödyntämistä sekä tietoturvayhtiöiden verkkokirjoituksien ja -julkaisujen käyttöä tutkimuskohteena itsessään sen sijaan, että näitä olisi hyödynnetty tutkimuskirjallisuusmaisesti muuta tutkimuskysymyksiin vastausten etsintää tukemassa. Suurimmaksi haasteeksi ja kipukohdaksi puolestaan osoittautui tutkimusmenetelmäksi valittu

habermasilainen diskurssianalyysi suhteessa tutkimusaineistoon. Aiemmassa tutkimuksessa, josta otin työhöni mallia, habermasilaista diskurssianalyysia oli hyödynnetty tietojärjestelmähankkeen uutisoinnin sekä tietoturvapolitiikkojen analysointiin. Näistä ensimmäisessä analyysin fokuksena oli median uutisoinnissaan hankkeesta painottamat puolet verrattuna "kokonaiseen" kuvaan hankkeen hyödyistä ja haitoista. Jälkimmäisessä tutkimuksessa puolestaan habermasilaisella diskurssianalyysilla etsittiin tietoturvapolitiikoista niiden sisältämiä ideologioita ja hegemonioita. Omassa tutkielmassani pyrin tasapainoilemaan näiden kahden lähestymistavan välillä, mutta se osoittautui haasteelliseksi.

Eniten pohdintaa tutkimusmenetelmän soveltamisen osalta aiheutti Habermasin totuuden pätevyysvaatimus. Aiemmassa habermasilaista diskurssianalyysia hyödyntäneessä tutkimuksessa tätä pätevyysvaatimusta on tarkasteltu etsien esitettyjen väitteiden taustalta löytyviä perusteita ja todisteita. Tällaisen aineistossa sanotun taustalla olevan "totuuden" olemassaolo, jota vasten arviointi tehdään, ei kuitenkaan mielestäni ole konstruktionistiselle tutkimukselle mielekäs lähtökohta. Esimerkiksi läpi tutkimusaineistoni kulkenutta väittämää, että COVID-19-pandemia on ollut kyberturvallisuuden vaikutusta lisännyt ja kiihdyttänyt tapahtuma, voitaisiin arvioida tutkimalla todisteita esimerkiksi tilastollisesti kasvaneiden tietoturvatapahtumien määrästä. Jos tapahtumien määrä olisi kasvanut, niin voitaisiin puolestaan tehdä johtopäätös, että kyllä, kyberturvallisuuden merkitys on korostunut ja kiihtynyt ja aineistossa sanottu on "totta". Kuitenkin yhtä lailla tällaisten tilastojen pohjalta voitaisiin todeta, että kyllä, tietoturvatapausten määrä näyttää kasvaneen COVID-19-pandemian myötä, mutta teillä ei pitäisi olla syytä huoleen, jos jatkatte toimintaanne nykyisten tietoturvakontrollienne mukaan. Myös tämänkään väittämän ja tulkinnan tilastojen pohjalta ei voitaisi sanoa olevan epätotuudenmukaista.

Tästä johtuen diskursseja analysoitaessa niiden "totuudellisuuden" arviointi ei ole mielekästä ainakaan kaikilta osin. Sen sijaan analyysin tehtävänä tulisi ennemminkin olla sen tarkastelu, mitkä puolet kielenkäytössä korostuvat ja minkä kustannuksella, ja mitä merkityksiä ja "sosiaalisia" totuuksia kyseinen kielenkäyttö tuottaa. Habermasilainen diskurssianalyysi tarjoaa toki myös tähän lähtökohtia, mutta vielä pidemmälle ja syvemmälle sosiaalisia totuuksia tarkastelevassa analyysissa voisi päästä esimerkiksi narratiivianalyysia tai jotakin muuta kriittisen diskurssianalyysin menetelmää käyttämällä.

Yleisesti ottaen diskurssianalyyttiselle tutkimukselle voidaan kritiikiksi lukea tapa, jolla aineistoa luetaan "kuin piru Raamattua" -henkisesti. Tekstejä analysoiva tutkija kiinnittää huomionsa jokaiseen sanamuotoon ja välimerkkiin, kun taas tekstin kirjoittanut taho, kuten tietoturvayhtiöiden julkaisujen kohdalla, on hyvinkin voinut kirjoittaa tekstin aikataulupaineissa ja kiireessä viimeiseksi työkseen ennen viikonloppuvapaille lähtöä, kun sellainen tuli esimiehelle luvattua. Tästä seurauksena ovat mahdolliset aineiston ja johtopäätösten sisältöä koskevat ylitulkinnat ja sieltä löytyvien merkitysten ylikorostaminen. Ylitulkinnan riski vähenee sitä mukaa, mitä suuremmasta tutkimusaineistomäärästä on kyse. Tämän takia valitsemaani tutkimusaihetta olisi jatkon kannalta aineiston osalta

paikallaan laajentaa sen vahvistamiseksi, pätevätkö tekemäni havainnot myös laajemmin kuin tarkastelemani kahden tietoturvayhtiön osalta.

Tutkimusaiheeni analyysia voitaisiin jatkossa myös viedä pidemmälle ottamalla mukaan kvantitatiivisia menetelmiä, esimerkiksi systemaattisesti laskemalla aineistossa käytettyjä sanoja, jotka rikastaisivat ymmärrystä tutkittavasta aiheesta. Tämä edellyttäisi tähän tarkoitettujen teknisten työkalujen ottamista mukaan osaksi tutkimusprosessia. Pro gradu -tutkielman kohdalla en näin tehnyt, koska sanojen lukumäärän ja toistuvuuden sijaan ensisijaisena tutkimuksellisena mielenkiinnon kohteena olivat sanojen ja ilmaisujen sisältämät merkitykset niiden lukumäärän sijaan.

8.3 Jatkotutkimus

Pro gradu -tutkielmani havaintoihin pohjautuvan jatkotutkimuksen osalta olisi kiinnostavaa ennen kaikkea selvittää sitä, miten tietoturvakonsultointiyhtiöiden COVID-19-pandemiaa koskeva diskurssi on otettu heidän kohdeyleisönään olevissa organisaatioissa vastaan. Tutkielmassani on tarkasteltu ja kuvattu sitä, millainen tämä diskurssi on, mutta merkittävää lisäarvoa tutkimusteemalla toisi analyysi, jossa käytäisiin esimerkkiasiakasyritysten kautta läpi, onko tämä sama diskurssi omaksuttu niissä ja millaisiin toimenpiteisiin se on johtanut. Lisäksi koska tutkielmani tarkastelun kohteena oli vain kaksi tietoturvayhtiötä, olisi hyödyllistä tutkia tätä diskurssia myös muiden tietoturvapalveluita tarjoavien yhtiöiden osalta yhtäläisyyksien ja mahdollisten erojen löytämiselle.

Ylipäätään koen, että turvallisuudentutkimuksen suuntauksen, jossa huomio kiinnitetään käytettyyn kieleen, siinä oleviin merkityksiin ja näiden merkitysten ymmärtämiseen, suosion lisääntymisestä myös kyberturvallisuuden tutkimuksen puolella olisi tieteenalalle hyötyä. Kansainvälisten suhteiden saralla turvallisuutta tutkivat tutkijat ovat enenevässä määrin lisäämässä kiinnostustaan myös kyberturvallisuuteen. Yhteistyö näiden ja kyberturvallisuuteen teknisemmältä kannalta perehtyneiden tutkijoiden välillä voisi tuoda mukanaan merkittäviä löydöksiä, jotka auttaisivat meitä vielä paremmin ymmärtämään ja hahmottamaan kyberturvallisuuden merkitystä turvallisuuden eri kerroksilla yksilöistä kansainväliseen politiikkaan.

LÄHTEET

TIETOTURVAKONSULTOINTIYHTIÖIDEN JULKAISUT

D1. (17.6.2020). New World, New Risk – How COVID-19 Is Transforming Business for the Next Normal. Haettu osoitteesta https://www2.deloitte.com/global/en/blog/responsible-business-blog/2020/how-covid-19-is-transforming-business-for-the-next-normal.html.

D2. (3.6.2020). COVID-19 Supercharges Cyber. Haettu osoitteesta https://www2.deloitte.com/global/en/blog/responsible-business-blog/2020/covid-19-supercharges-cyber.html.

D3. (30.7.2020). The Acceleration of Digitization as a Result of COVID-19. Haettu osoitteesta https://www2.deloitte.com/global/en/blog/responsible-business-blog/2020/acceleration-of-digitization-as-result-of-covid-19.html.

D4. (15.10.2020). States at risk: The cybersecurity imperative in uncertain times. Haettu osoitteesta https://www2.deloitte.com/us/en/insights/industry/public-sector/nascio-survey-government-cybersecurity-strategies.html.

D4b. (15.10.2020). 2020 Deloitte-NASCIO Cybersecurity Stydy. States at risk: the cybersecurity imperative in uncertain times. Haettu osoitteesta https://www2.deloitte.com/us/en/insights/industry/public-sector/nascio-survey-government-cybersecurity-strategies.html.

D5. (23.9.2020). Rebooting risk management. Making risk relevant in a world remade by COVID-19. Haettu osoitteesta https://www2.deloitte.com/us/en/insights/economy/covid-19/risk-management-during-covid-19.html.

D5b. (23.9.2020). D5. (23.9.2020). Rebooting risk management. Making risk relevant in a world remade by COVID-19 (PDF-raportti). Haettu osoitteesta https://www2.deloitte.com/us/en/insights/economy/covid-19/risk-management-during-covid-19.html.

D6. (24.7.2020). Reshaping the cybersecurity landscape. How digitization and the COVID-19 pandemic are accelerating cybersecurity needs at many large financial institutions. Haettu osoitteesta https://www2.deloitte.com/us/en/insights/industry/financial-services/cybersecurity-maturity-financial-institutions-cyber-risk.html.

P1. (2020). Cyber security strategy 2021 – An urgent business priority. Haettu osoitteesta https://www.pwc.co.uk/issues/cyber-security-services/insights/cyber-security-strategy-2021.html.

P1b. (2020). Global Digital Trust Survey 2021. Haettu osoitteesta https://www.pwc.com/us/en/services/consulting/cybersecurity-privacy-forensics/library/global-digital-trust-insights.html.

P2. (2020). How fake news has exploited COVID-19. Haettu osoitteesta https://www.pwc.co.uk/issues/crisis-and-resilience/covid-19/how-fake-news-has-exploited-covid19-cyber.html.

P3. (1.7.2020). How to maintain your cyber security awareness programme with a remote workforce. Haettu osoitteesta https://pwc.blogs.com/cyber_security_updates/2020/07/how-to-maintain-your-cyber-security-awareness-programme-with-a-remote-workforce.html.

P4. (2020). Why has there been an increase in cyber security incidents during COVID-19? Haettu osoitteesta https://www.pwc.co.uk/issues/crisis-and-resilience/covid-19/why-an-increase-in-cyber-incidents-during-covid-19.html.

P5. (2020). SWIFT CSP controls and remote working practices – This might be the time to revisit SWIFT CSP controls in the context of remote working practices due to COVID-19. Haettu osoitteesta https://www.pwc.co.uk/industries/financial-services/regulation/swift-customer-security-programme/swift-csp-controls-remote-working-covid-19.html.

P6. (2020). Digital Identity supports a secure remote digital workforce during COVID-19. Haettu osoitteesta https://www.pwc.co.uk/issues/crisis-and-resilience/covid-19/digital-identity-supports-a-secure-remote-digital-workforce-duri.html.

P6b. (2020) Digital Identity supports a secure remote digital workforce during COVID-19. Haettu osoitteesta https://www.pwc.co.uk/issues/crisis-and-resilience/covid-19/digital-identity-supports-a-secure-remote-digital-workforce-duri.html.

P7. (2020). COVID-19: Making remote work productive and secure. Haettu osoitteesta https://www.pwc.com/us/en/library/covid-19/global-privacy-impact-assessment.html.

P8. (2020). How to protect your companies from rising cyber attacks and fraud amid the COVID-19. Haettu osoitteesta https://www.pwc.com/us/en/library/covid-19/cyber-attacks.html.

P9. (24.3.2020). How to manage the impact of COVID-19 on cyber security. Haettu osoitteesta https://www.pwc.co.uk/issues/crisis-and-resilience/covid-19/how-to-manage-the-impact-of-covid-19-on-cyber-security.html.

P9b. (20.3.2020). Managing the impact of COVID-19 on cyber security. Haettu osoitteesta https://www.pwc.co.uk/issues/crisis-and-resilience/covid-19/how-to-manage-the-impact-of-covid-19-on-cyber-security.html.

TUTKIMUSKIRJALLISUUS JA MUUT LÄHTEET

Adams, R.J., Smart, P. & Huff, A.S. (2017). Shades of Grey: Guidelines for Working with the Grey Literature in Systematic Reviews for Management and Organizational Studies. *International Journal of Management Reviews, 19(4),* 432-454.

Anderson, B. (2006). *Kuvitellut yhteisöt: nationalismin alkuperän ja leviämisen-tarkastelua* (suom. Kuortti, J.). Tampere: Vastapaino.

Asonye, C. (5.6.2020). There's nothing new about the 'new normal'. Here's why. Haettu osoitteesta https://www.weforum.org/agenda/2020/06/theres-nothing-new-about-this-new-normal-heres-why/.

Bay, M. (2016). What is cybersecurity? In search of an encompassing definition for the post-Snowden era. *French Journal for Media Research.* Julkaistu verkossa http://frenchjournalformediaresearch.com/lodel-1.0/main/index.php?id=988.

Bazeley, P. (2021). *Qualitative Data Analysis. Practical Strategies* (2. painos). Lontoo: SAGE.

Berger, P.L. & Luckmann, T. (1996). *Todellisuuden sosiaalinen rakentuminen* (suom. Raiskila, V.). Helsinki: Kirjapaino-Oy Like.

Burr, V. (2003). *Social Constructionism* (2. painos). Lontoo: Routledge.

Butler, J. (2006). *Hankala sukupuoli: feminismi ja identiteetin kumous* (suom. T. Pulkkinen, L-M. Rossi). Helsinki: Gaudeamus.

Buzan, B., Waever. O. & de Wilde, J. (1998). *Security: A New Framework for Analysis*. Lontoo: Lynne Rienner Publishers, Inc.

Campbell, D. (1998). *Writing Security. United States Foreign Policy and the Politics of Identity. Revised Edition.* Manchester: Manchester University Press.

Check Point. (18.1.2021). Protecting Against a Rapidly Spreading Cyber Pandemic. Haettu osoitteesta https://www.checkpoint.com/cybersecurity-protect-from-cyber-pandemic/.

Chouliaraki, L. & Fairclough, N. (1999). *Discourse in Late Modernity – Rethinking Critical Discourse Analysis.* Edinburgh: Edinburgh University Press.

Christensen, K.K. & Liebetrau, T. (2019). A new role for 'the public'? Exploring cyber security controversies in the case of WannaCry. *Intelligence and National Security, 34(3),* 395-408.

Cukier, W., Bauer, R. & Middleton, C. (2004). Applying Habermas Validity Claims as a Standard for Critical Discourse Analysis. *IFIP International Federation for Information Processing.* Tammikuu. Konferenssipaperi.

Cukier, W., Ngwenyama, O., Bauer, R. & Middleton, C. (2009). A critical analysis of media discourse on information technology: preliminary results of a proposed method for critical discourse analysis. *Information Systems Journal 19,* 175-196.

Deutschmann, C. (1996). Money as a Social Construction: On the Actuality of Marx and Simmel. *Thesis Eleven, 47(1)*, 1-19.

Edgar, A. (2005). *The philosophy of Habermas.* Chesham: Acumen.

Eiriksen, E.O. & Weigård, J. (2003). *Understanding Habermas – Communicating Action and Deliberative Democracy*. Lontoo: Continuum.

Fairclough, N. (1997). *Miten media puhuu* (suom, V. Blom & K. Hazard). Tampere: Vastapaino.

Forrester. (2019). The Forrester Wave: Global Cybersecurity Consulting Providers, Q2 2019. Saatavilla osoitteesta https://www.forrester.com/report/The+Forrester+Wave+Global+Cybersecurity+Consulting+Providers+Q2+2019/-/E-RES146436.

Foucault, M. (1980). *Tarkkailla ja rangaista* (suom, E. Nivanka). Helsinki: Kustannusosakeyhtiö Otava.

Foucault, M. (2010). *Seksuaalisuuden historia* (suom, K. Sivenius, 2. uudistettu laitos). Helsinki: Gaudeamus.

Gartner. (6.6.2018). Gartner Top 10 Security Projects for 2018. Haettu osoitteesta https://www.gartner.com/smarterwithgartner/gartner-top-10-security-projects-for-2018/.

Gartner. (18.6.2019). Gartner Top 10 Security Projects for 2019. Haettu osoitteesta https://www.gartner.com/smarterwithgartner/gartner-top-10-security-projects-for-2019/.

Graber, S.M. (2017). War of perception: a Habermasian discourse analysis of human shield newspaper reporting during the 2014 Gaza War. *Critical Studies in Media Communication, 34(3),* 297-307.

Graham, P. & Luke, A. (2011). Critical Discourse Analyis and Political Economy of Communication: Understanding the New Corporate Order. *Cultural Politics, 7(1),* 103-132.

Gralewski, M. (2011). The Philosophical Underpinnings of Social Constructionist Discourse Analysis. *Lodz Papers in Pragmatics, 7(1)*, 155-171.

Habermas, J. (1984). *The Theory of Communicative Action. Volume 1: Reason and the Rationalization of Society* (engl. T. McCarthy). Lontoo: Heinemann.

Habermas, J. (1989). *The Theory of Communicative Action. Volume 2: Lifeworld and System: A Critique of Functionalist Reason* (engl. T. McCarthy). Cambridge: Polity Press.

Hansen, L. & Nissenbaum, H. (2009). Digital Disaster, Cyber Security, and the Copenhagen School. *International Studies Quarterly*, 53, 1155-1175.

Harvey, J. & Branco-Illodo, I. (2020). Why Cryptocurrencies Want Privacy: A Review of Political Motivations and Branding Expressed in "Privacy Coin" Whitepapers. *Journal of Political Marketing, 19(1-2),* 107-136.

Hirsjärvi, S., Remes, P. & Sajavaara, P. (2007). *Tutki ja kirjoita* (13. osin uudistettu painos). Helsinki: Kustannusosakeyhtiö Tammi.

Hodges, A. (2011). *The "War on Terror" Narrative – Discourse and Intertextuality in the Construction and Contestation of Sociopolitical Reality*. Oxford: Oxford University Press.

Hynek, N. & Chandler, D. (2013). No emancipatory alternative, no critical security studies. *Critical Studies on Security*, *1(1)*, 46-63.

Jackson, R. (2005). *Writing the War on Terrorism: Language, Politics and Counter-terrorism*. Manchester: Manchester University Press.

Jantunen, S. & Huhtinen, A-M. (2011). American perspectives on cyber and security: Coining the linguistic tradition. *Journal of Information Warfare, 10(3)*, 1-15.

Johnstone, B. (2008). *Discourse Analysis* (2. painos). Oxford: Blackwell Publishing.

Jokinen, A. (2002). Diskurssianalyysin suhde sukulaistraditioihin. Teoksessa A. Jokinen, K. Juhila & E. Suoninen, *Diskurssianalyysi liikkeessä* (s. 37-53). Jyväskylä: Gummerus Kirjapaino Oy.

Jokinen, A. & Juhila, K. (2002). Diskurssianalyyttisen tutkimuksen kartta. Teoksessa A. Jokinen, K. Juhila & E. Suoninen, *Diskurssianalyysi liikkeessä* (s. 54-100). Jyväskylä: Gummerus Kirjapaino Oy.

Jokinen, A., Juhila, K. & Suoninen. E. (2002). *Diskurssianalyysi liikkeessä* (2. painos). Jyväskylä: Gummerus Kirjapaino Oy.

Juhila, K. (2002). Tutkijan positiot. Teoksessa A. Jokinen, K. Juhila & E. Suoninen, *Diskurssianalyysi liikkeessä* (s. 201-232). Jyväskylä: Gummerus Kirjapaino Oy.

Juhila, K. & Suoninen, E. (2002). Kymmenen kysymystä diskurssianalyysista. Teoksessa A. Jokinen, K. Juhila & E. Suoninen, *Diskurssianalyysi liikkeessä* (s. 233-252). Jyväskylä: Gummerus Kirjapaino Oy.

Kangas, R. (1989). *Jürgen Habermasin kommunikatiivisen toiminnan teoria* (2. painos). Helsinki: Tutkijaliitto.

Koerber, A., Arnet, E.J. & Cumbie, T. (2008). Distortion and Politics of Pain Relief. A Habermasian Analysis of Medicine in the Media. *Journal of Business and Technical Communication, 22(3),* 364-391.

Lacy, M. & Prince, D. (2018): Securitization and the global politics of cybersecurity. *Global Discourse, 8(1),* 100-115.

Liebetrau, T. & Christensen, K.K. (2021). The ontological politics of cyber security: Emerging agencies, actors, sites, and spaces. *European Journal of International Security, 6(1),* 25-43.

Lock, A. & Strong, T. (2011). *Social Constructionism: Sources and Stirrings in Theory and Practice* (uusintapainos). Cambridge: Cambridge University Press.

Lyytinen, K. (1992). Information Systems and Critical Theory. Teoksessa M. Alvesson & H. Willmott, *Critical Management Studies* (s. 159-180). Lontoo: SAGE Publications.

Lyytinen, K. & Hirschheim, R. (1988). Information systems as rational discourse: an application of Habermas's theory of communicative action. *Scandinavian Journal of Management Studies, 4(1/2),* 19-30.

Lämsä, A-M. (2014). *Diskurssianalyysi empiirisen tutkimuksen näkökulmasta*. Haettu osoitteesta https://metodix.fi/2014/05/19/lamsa-diskurssianalyysi-empiirisen-tutkimuksen-nakokulmasta/.

O'Gara, C. (23.9.2019). 'Stop Selling Fear,' CISA Director Tells Cybersecurity Community. Haettu osoitteesta https://www.secureworldexpo.com/industry-news/cybersecurity-leaders-stop-selling-fear.

Peoples, C. & Vaughan-Williams, N. (2010). *Critical Security Studies. An Introduction.* Lontoo: Routledge.

Pieters, W. (2011). The (Social) Construction of Information Security. *The Information Society, 27(5),* 326-335.

Poutanen, M. (2016). Kriisien poliittinen ulottuvuus ja turvallistamisteoria tapana hahmottaa kriisejä. *Kriisi 1/2016.* Haettu osoitteesta https://hybrislehti.net/kriisien-poliittinen-ulottuvuus-ja-turvallistamisteoria-tapana-hahmottaa-kriisej.

Rantapelkonen, J. (2006). *The Narrative Leadership of War.* Helsinki: National Defence University, Department of Leadership and Management Studies.

Rose, S., Borchert, O., Mitchell, S. & Connelly, S. (2020). *Zero Trust Architecture. NIST Special Publication 800-207.* Haettu osoitteesta https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-207.pdf.

Rothstein, H.R. & Hopewell, S. (2009). Grey Literature. Teoksessa H. Cooper, L.V. Hedges & J.C. Valentine, *The Handbook of Research Synthesis and Meta-Analysis* (s. 103-125). New York: Russell Sage Foundation.

Stahl, B.C., Doherty, N.F. & Shaw, M. (2012). Information security policies in the UK healthcare sector: a critical evaluation. *Information Systems Journal, 22(1),* 77-94.

Stankiewicz, P. (2008). Invisible Risk. The Social Construction of Security. *Polish Sociological Review*, *161(1)*, 55-72.

Suoninen, E. (2002). Näkökulmia sosiaalisen todellisuuden rakentumiseen. Teoksessa A. Jokinen, K. Juhila & E. Suoninen, *Diskurssianalyysi liikkeessä* (s. 17-36). Jyväskylä: Gummerus Kirjapaino Oy.

Sweet, P. (24.5.2019). Big Four dominate cyber security job space. Haettu osoitteesta https://www.accountancydaily.co/big-four-dominate-cyber-security-job-space.

Timotijevic, J. (2020). *Society's 'new normal'? The role of discourse in surveillance and silencing of dissent during and post Covid-19.* Haettu osoitteesta https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3608576.

Todor, R-D. (2014). The Importance of Branding and Rebranding for Strategic Marketing. *Bulletin of the Transilvania University of Braşov, Series V: Economic Sciences, 7(56)*, 59-64.

Van Dijk, T.A. (1995). Aims of Critical Discourse Analysis. *Japanese Discourse, 1(1)*. 17-27.

Van Dijk, T. A. (2001). Multidisciplinary CDA a plea for diversity. Teoksessa R. Wodak & M. Meyer (toim.), *Methods of Critical Discourse Analysis* (s. 95-120). Lontoo: SAGE Publications.

Vuori, J. (2004). Turvallistaminen totalitaarisessa poliittisessa järjestelmässä – Makrotason mallin ja mikrotason analyysin yhdistämistä. *Kosmopolis*, *34(3)*, 4-28.

Vuori, J. (2011). *How to Do Security with Words. A Grammar of Securitisation in the People's Republic of China* (väitöskirja, Turun yliopisto).

Wall, J.D., Stahl, B.C. & Salam, A.F. (2015). Critical Discourse Analysis as a Review Methodology: An Empirical Example. *Communications of the Association for Information Systems, 37(11)*. 257-285.

Wang, J., Chaudhury, A. & Rao, R. (2008). Research Note – A Valuet-at-Risk Approach to Information Security Investment. *Information Systems Research*, *19(1)*, 106-120.

WHO. (31.7.2020). Rolling updates on coronavirus disease (COVID-19). Haettu osoitteesta https://www.who.int/emergencies/diseases/novel-coronavirus-2019/events-as-they-happen.

Wodak, R. (2001). What CDA is about – a summary of its history, important concepts and its developments. Teoksessa R. Wodak & M. Meyer (toim.), *Methods of Critical Discourse Analysis* (s. 1-13). Lontoo: SAGE Publications.

Wynne, B. (2002). Risk and Environment as Legitimatory Discourses of Technology: Reflexivity Inside Out? *Current Sociology, 50(3)*, 459-477.